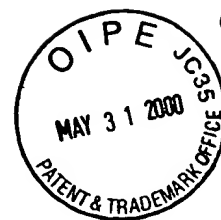


日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 3月 2日

出 願 番 号

Application Number:

特願2000-057077

出 願 人

Applicant (s):

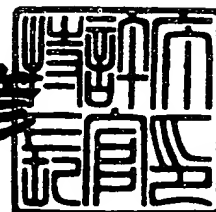
キヤノン株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 4月14日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3027116

【書類名】 特許願

【整理番号】 4184060

【提出日】 平成12年 3月 2日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G06F 15/00  
H04N 7/00

【発明の名称】 画像処理装置、方法及びシステム、並びに撮像装置、撮  
像方法、コンピュータ読み取り可能な記憶媒体

【請求項の数】 42

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 若尾 聡

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 岩村 恵市

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キャノン株式会社

【代表者】 御手洗 富士夫

【電話番号】 03-3758-2111

【代理人】

【識別番号】 100090538

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【弁理士】

【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100096965

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 内尾 裕一

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100110009

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 青木 康

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100069877

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 丸島 儀一

【電話番号】 03-3758-2111

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第 63174号

【出願日】 平成11年 3月10日

【手数料の表示】

【予納台帳番号】 011224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9908388

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項 1】 デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする画像処理装置。

【請求項 2】 請求項 1 において、前記演算手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な演算を行うことを特徴とする画像処理装置。

【請求項 3】 請求項 1 若しくは 2 において、前記生成手段は、前記演算手段の演算結果に対して、逆演算の困難な演算を行うことを特徴とする画像処理装置。

【請求項 4】 請求項 3 において、前記逆演算の困難な演算は、ハッシュ関数を用いた演算であることを特徴とする画像処理装置。

【請求項 5】 請求項 3 において、前記一方向性関数は、共通鍵暗号を実現する演算であることを特徴とする画像処理装置。

【請求項 6】 請求項 1 ～ 5 の何れかにおいて、前記生成手段は、前記デジタル画像毎に、該デジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項 7】 請求項 1 ～ 6 の何れかにおいて、前記生成手段は、前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するため署名データを生成するプログラムに従って前記デジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項 8】 請求項 1 ～ 7 の何れかにおいて、前記秘密情報は、前記画像処理装置を識別するための情報であることを特徴とする画像処理装置。

【請求項 9】 請求項 1 ～ 7 の何れかにおいて、前記秘密情報は、前記画像

処理装置と接続可能な外部装置を識別するための情報であることを特徴とする画像処理装置。

【請求項 1 0】 請求項 1 ～ 7 の何れかにおいて、前記秘密情報は、前記画像処理装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする画像処理装置。

【請求項 1 1】 請求項 1 ～ 1 0 の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記画像処理装置に接続された外部装置に演算させることを特徴とする画像処理装置。

【請求項 1 2】 請求項 1 ～ 1 1 の何れかにおいて、前記デジタル画像は、圧縮符号化されていることを特徴とする画像処理装置。

【請求項 1 3】 請求項 1 ～ 1 2 の何れかにおいて、前記画像処理装置は更に、前記デジタル画像を生成する撮像部を具備することを特徴とする画像処理装置。

【請求項 1 4】 請求項 1 ～ 1 3 の何れかにおいて、前記画像処理装置は更に、前記デジタル画像と前記署名データとを出力可能なデジタルインタフェースを具備することを特徴とする画像処理装置。

【請求項 1 5】 請求項 1 ～ 1 4 の何れかにおいて、前記画像処理装置は更に、前記前記デジタル画像データと前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする画像処理装置。

【請求項 1 6】 デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする画像処理装置。

【請求項 1 7】 請求項 1 6 において、前記演算手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な第 1 の演算を行うことを特徴とする画像処理装置。

【請求項 1 8】 請求項 1 7 において、前記演算手段は、前記第 1 の演算の結果に対して、一方向関数を用いた第 2 の演算を行うことを特徴とする画像処理

装置。

【請求項 1 9】 請求項 1 6 ～ 1 8 の何れかにおいて、前記画像処理装置は、前記デジタル画像毎に、該デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項 2 0】 請求項 1 6 ～ 1 9 の何れかにおいて、前記検出手段は、前記演算手段の出力と前記署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出するプログラムに従って前記デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項 2 1】 請求項 1 6 ～ 2 0 の何れかにおいて、前記画像処理装置は更に、前記検出手段の検出結果を表示する表示手段を具備することを特徴とする画像処理装置。

【請求項 2 2】 デジタル画像と秘密情報とを用いて所定の演算を行う第 1 の演算手段と、

前記第 1 の演算手段の出力を用いて、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第 1 の画像処理装置と、

前記デジタル画像と前記秘密情報とを用いて所定の演算を行う第 2 の演算手段と、

前記第 2 の演算手段の出力と前記署名データとを比較して該デジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第 2 の画像処理装置とにより構成することを特徴とする画像処理システム。

【請求項 2 3】 デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする画像処理方法。

【請求項 2 4】 デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理方法。

【請求項 2 5】 デジタル画像と秘密情報とを用いて所定の演算を行う手

順と、

該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 2 6】 デジタル画像と秘密情報とを用いて所定の演算を行う手順と、

該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 2 7】 デジタル画像を生成する撮像手段と、

前記デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする撮像装置。

【請求項 2 8】 請求項 2 7 において、前記生成手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な第 1 の演算を行うことを特徴とする画像処理装置。

【請求項 2 9】 請求項 2 8 において、前記生成手段は、前記第 1 の演算の結果に対して一方向関数を用いた第 2 の演算を行うことを特徴とする画像処理装置。

【請求項 3 0】 請求項 2 9 において、前記一方向性関数は、ハッシュ関数であることを特徴とする撮像装置。

【請求項 3 1】 請求項 2 9 において、前記一方向性関数は、共通鍵暗号を実現する関数であることを特徴とする撮像装置。

【請求項 3 2】 請求項 2 9 において、前記生成手段は、前記撮像手段が前記デジタル画像を生成する毎に、該デジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項 3 3】 請求項 2 7 ～ 3 2 の何れかにおいて、前記生成手段は、前記撮像手段により生成されたデジタル画像と秘密情報とを用いて所定の演算を

行い、該デジタル画像に対する不正な処理を検出するための署名データを生成するプログラムに従って前記デジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項 3 4】 請求項 2 7 ～ 3 3 の何れかにおいて、前記秘密情報は、前記撮像装置を識別するための情報であることを特徴とする撮像装置。

【請求項 3 5】 請求項 2 7 ～ 3 3 の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を識別するための情報であることを特徴とする撮像装置。

【請求項 3 6】 請求項 2 7 ～ 3 3 の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする撮像装置。

【請求項 3 7】 請求項 2 7 ～ 3 6 の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記撮像装置に接続された外部装置に演算させることを特徴とする撮像装置。

【請求項 3 8】 請求項 2 7 ～ 3 7 の何れかにおいて、前記デジタル画像は、圧縮符号化されていることを特徴とする撮像装置。

【請求項 3 9】 請求項 2 7 ～ 3 8 の何れかにおいて、前記撮像装置は更に、前記デジタル画像と前記署名データとを出力可能なデジタルインタフェースを具備することを特徴とする撮像装置。

【請求項 4 0】 請求項 2 7 ～ 3 9 の何れかにおいて、前記撮像装置は更に、前記前記デジタル画像と前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする撮像装置。

【請求項 4 1】 デジタル画像を撮像し、  
該デジタル画像と秘密情報とを用いて所定の演算を行い、  
該デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする撮像方法。

【請求項 4 2】 撮像部により撮像されたデジタル画像と、秘密情報とを用いて所定の演算を行う手順と、

該デジタル画像に対する不正な処理を検出するための署名データを生成する

手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体に関し、特に、デジタル画像情報の著作権を保護するための技術に関するものである。

【0002】

【従来の技術】

近年、撮影した画像を従来の銀塩写真や8mmフィルムに記録するのではなく、デジタルデータとして記録媒体に記録する画像入力装置（例えば、デジタルカメラ）が実用化されている。

【0003】

【発明が解決しようとする課題】

ところが、通常、デジタルデータは、アナログデータと異なり加工が容易で、修正、改竄、偽造、合成等を簡単に行うことができる。このため、デジタルデータは、銀塩写真等と比較して信憑性が低く、証拠能力に乏しいという問題があった。

【0004】

このような問題を解決するために、デジタルデータに対する修正、改竄、偽造、合成等を検出するための技術が提案されている。例えば、この技術の一例として、ハッシュ関数と公開鍵暗号方式とを組み合わせたシステムが提案されている。

【0005】

以下、図28を用いて従来のシステムを説明する。公開鍵暗号方式とは、暗号鍵と復号鍵とが異なり、暗号鍵を公開し、復号鍵を秘密に保持する方式である。

【0006】

まず、送信側（出力側）の構成と動作について説明する。

- ①デジタルデータMをハッシュ関数Hを用いて圧縮し、一定長の出力hを演算する。
- ②暗号鍵K<sub>e</sub>を用いて上述のhを暗号化し、出力sを求める。この出力sをデジタル署名データと呼ぶ。
- ③出力回路は、デジタル署名データsとデジタルデータMとを一組として出力する。

【 0 0 0 7 】

次に、受信側（検出側）構成と動作について説明する。

- ④デジタルデータMとそれに対応するデジタル署名データsとを入力する。
- ⑤デジタル署名データsを暗号鍵K<sub>e</sub>に対応する復号鍵K<sub>d</sub>で復号し、出力h'を生成する。
- ⑥デジタルデータMを送信側と同じハッシュ関数Hを用いて演算し、出力h'を求める。
- ⑦比較回路は、⑤で求めた出力h'と⑥で求めた出力h'とを比較し、一致すれば入力されたデジタルデータMを不正な処理のされていない正当なデータであると判断し、不一致であれば不正な処理のされたデータと見なす。

【 0 0 0 8 】

このように従来のシステムでは、ハッシュ関数Hと暗号鍵K<sub>e</sub>とにより生成したデジタル署名データsを用いて、デジタルデータMに対する修正、改竄、偽造、合成等を検出していた。

【 0 0 0 9 】

しかしながら、上述のシステムには次のような問題がある。

【 0 0 1 0 】

まず、公開鍵暗号方式の暗号化回路及びその復号化回路は、回路構成が複雑であり、小型化が難しいという問題がある。また、それらの回路の演算量は膨大であり、処理時間が長くなるという問題もある。特に、公開鍵暗号方式は、べき乗演算と剰余演算とが必要であり、共通鍵暗号方式（暗号鍵と復号鍵とが同一となる暗号方式）に比べて演算が複雑且つ膨大となるため、処理速度の高速化が大変難しい。つまり、従来のシステムでは、処理速度の高速化とシステムの小型化の

双方を両立させることは難しいという問題がある。

【 0 0 1 1 】

又、処理速度を早くするためには、より高性能のCPU（中央演算処理装置）とより大容量のメモリとを用いて、ハードウェアの性能を向上させる必要がある。しかしながら、このような構成では、システム全体の大規模化やコストアップを招くだけであり、安価で小型で高速なシステムをユーザに提供することはできない。

【 0 0 1 2 】

以上の背景から本出願の発明の目的は、デジタルデータの著作権を保護を、簡単な構成で、安価に且つ安全に実現することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【 0 0 1 3 】

【課題を解決するための手段】

上述のような目的を達成するために、本発明の画像処理装置は、デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【 0 0 1 4 】

又、本発明の画像処理装置は、デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする。

【 0 0 1 5 】

又、本発明の画像処理システムは、デジタル画像と秘密情報とを用いて所定の演算を行う第1の演算手段と、前記第1の演算手段の出力を用いて、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第1の画像処理装置と、前記デジタル画像と前記秘密情報とを用いて所定の演算を行う第2の演算手段と、前記第2の演算手段の出力と前記署名デ

ータとを比較して該デジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第2の画像処理装置とにより構成することを特徴とする。

【0016】

又、本発明の画像処理方法は、デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【0017】

又、本発明の画像処理方法は、デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出することを特徴とする。

【0018】

又、本発明のコンピュータ読み取り可能な記憶媒体は、デジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0019】

又、本発明のコンピュータ読み取り可能な記憶媒体は、デジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0020】

又、本発明の撮像装置は、デジタル画像を生成する撮像手段と、前記デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【0021】

又、本発明の撮像方法は、デジタル画像を撮像し、該デジタル画像と秘密

情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【 0 0 2 2 】

又、本発明のコンピュータ読み取り可能な記憶媒体は、撮像部により撮像されたデジタル画像と、秘密情報とを用いて所定の演算を行う手順と、該デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【 0 0 2 3 】

【発明の実施の形態】

以下、本発明の画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体について図面を用いて詳細に説明する。

【 0 0 2 4 】

(基本構成)

まず、図 1 を用いて、各実施例に共通するデジタル画像検証システムの基本構成と処理手順とについて説明する。このシステムは、デジタル画像データからデジタル署名データを生成するデジタル画像入力装置 1 0 と、そのデジタル署名データを用いてデジタル画像データに対する不正な処理を検出する画像検証装置 2 0 とからなる。各装置は、ネットワーク（例えば、インターネット、電話回線網、移動体通信網等）、各機器に共通のデジタルインタフェース、取り外し可能な記憶媒体（例えば、光ディスク、磁気ディスク、光磁気ディスク、半導体メモリ等）を介して接続される。

【 0 0 2 5 】

尚、図 1 において、画像入力装置 1 0 と画像検証装置 2 0 とは、同一の秘密情報 S 1 2 を共有する。この秘密情報 S 1 2 は、読み出し専用の記録媒体等に記録され、外部に漏れることがないように管理する。

【 0 0 2 6 】

まず、画像入力装置 1 0 は、デジタル画像データ P 1 1 と秘密情報 S 1 2 とに基づいて、デジタル署名データ h 1 3 を生成する。具体的に説明すると、画像入力装置 1 0 は、秘密情報 S 1 2 を用いてデジタル画像データ P 1 1 に所定

の操作（例えば、付加、多重、或いは合成）を加えた後、その結果を一方向性関数（例えば、ハッシュ関数等の逆関数の生成が困難或いは不可能な関数）で演算し、その演算結果からデジタル署名データ  $h13$  を生成する。このデジタル署名データ  $h13$  は、対応するデジタル画像データ  $P11$  と共に一時的に記録され、必要に応じて外部出力される。

## 【 0 0 2 7 】

このような処理によって得られたデジタル署名データ  $h13$  は、デジタル画像データ  $P11$  と秘密情報  $S12$  とに対して固有の情報となる。従って、秘密情報  $S12$  と所定の操作とを知らなければ、デジタル画像データ  $P11$  に対応するデジタル署名データ  $h13$  を不正に作り出すことはできないため、デジタル署名データ  $h13$  に基づいてデジタル画像データ  $P11$  の正当性を安全に検証することができる。又、一方向性関数の性質により、デジタル署名データ  $h13$  から元のデータ（即ち、秘密情報  $S12$  を用いて所定の操作を加えたデジタル画像データ  $P11$ ）を知ることもしできないため、デジタル署名データ  $h13$  に基づいてデジタル画像データ  $P11$  の正当性（或いは、完全性（*integrality*）ともいう）を安全に検証することができる。

## 【 0 0 2 8 】

次に、画像検証装置 20 は、デジタル画像データ  $P'21$  と共にデジタル署名データ  $h'23$  を外部入力する。画像検証装置 20 は、デジタル画像データ  $P'21$  と秘密情報  $S22$ （上述の秘密情報  $S12$  と同一の情報である）とを用いて画像入力装置 10 と同様の処理を行い、デジタル署名データ  $h''24$  を生成する。

## 【 0 0 2 9 】

このデジタル署名データ  $h''24$  は、デジタル画像データ  $P'21$  と共に外部入力されたデジタル署名データ  $h'23$  と比較される。両者が一致した場合、画像検証装置 20 は、デジタル画像データ  $P'21$  を正当なデータであると判断する。一方、デジタル画像データ  $P'21$  が外部入力される前に不正に処理されていた場合、両者は不一致となる。この場合、画像検証装置 20 は、デジタル画像データ  $P'21$  を不正に処理されたデータであると判断する。

## 【 0 0 3 0 】

このような手順により、画像検証処装置 2 0 は、外部入力されたデジタル画像データ P' 2 1 に対して不正な処理（例えば、修正、改竄、偽造、合成等の改変処理）が施されているか否かを検出することができる。

## 【 0 0 3 1 】

以上のように、本実施例では、公開鍵暗号方式のような複雑な暗号化技術を用いることなく、簡単で安価な回路構成と少ない演算量で高速にデジタル署名データを生成することができる。そして、このデジタル署名データにより、デジタル画像データの著作権を保護し、該デジタル画像データに対する不正な処理（修正、改竄、偽造、合成等の改変処理）を確実に検出することができる。

## 【 0 0 3 2 】

次に、図 2 に示す画像入力装置 1 0 及び画像検証装置 2 0 の基本的な構成について詳細に説明する。

## 【 0 0 3 3 】

## （ 1 ） 画像入力装置の構成

図 2 は、画像入力装置 1 0 の構成の一例を示す図である。ここで、画像入力装置 1 0 は、デジタルカメラ、カメラ一体型デジタルレコーダ、スキャナ等の撮像機能を有する電子機器である。

## 【 0 0 3 4 】

図 2 において、撮像部 2 0 1 は、CCD やレンズ等からなり、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのデジタル画像データに変換する。作業用メモリ 2 0 2 は、デジタル画像データ等を一時的に保管し、デジタル画像データに対する高能率符号化処理、後述のデジタル署名データの生成等に使用される。

## 【 0 0 3 5 】

記録再生部 2 0 3 は、取り外し可能な記録媒体（例えば、光ディスク、磁気ディスク、光磁気ディスク、半導体メモリ等）に、撮像部 2 0 1 により生成され、高能率符号化されたデジタル画像データとそれに対応するデジタル署名データとを一組として記録する。駆動部 2 0 4 は、撮像部 2 0 1 や記録再生部 2 0 3

の機械的動作を制御する。

【 0 0 3 6 】

外部インタフェース部 2 0 5 は、ネットワーク（例えば、インターネット、電話回線網、移動体通信網等）に接続可能なデジタルインタフェースであり、デジタル署名データを付加したデジタル画像データを、所定の外部装置に送信する。

【 0 0 3 7 】

制御／演算部 2 0 6 は、ROM 2 0 7 に格納されている各種のプログラムに従って画像入力装置 1 0 全体の動作を制御する制御回路 2 1 0、デジタル画像データを高能率符号化する（例えば、DCT変換やウェーブレット変換されたデジタル画像データを量子化し、可変長符号化する）画像処理回路 2 1 1、後述のデジタル署名データの生成に必要なハッシュ関数演算や各種の演算処理を行う演算回路 2 1 2、デジタル署名データの生成に必要な秘密情報（例えば、画像入力装置 1 0 を識別するための ID 情報等）を格納するメモリ 2 1 3、演算回路 2 1 2 に必要な乱数を生成する乱数発生回路 2 1 4 を含む。

【 0 0 3 8 】

ROM 2 0 7 は読み出し専用メモリであり、画像入力装置 1 0 全体の動作を制御するプログラム、画像処理を制御するプログラム、デジタル署名データの生成処理を制御するプログラム等を格納している。操作部 2 0 8 は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部 2 0 6 に供給する。

【 0 0 3 9 】

（ 2 ）画像検証装置の構成

図 3 は、画像検証装置 2 0 の構成の一例を示す図である。ここで、画像検証装置 2 0 は、パーソナルコンピュータ、ワークステーション等の情報処理装置やそれらに接続可能な拡張ボードである。

【 0 0 4 0 】

図 3 において、外部インタフェース部 3 0 1 は、ネットワークからデジタル署名データを付加したデジタル画像データ（ここで、デジタル画像データは

、高能率符号化されている)を入力するデジタルインタフェースである。又、外部インタフェース部 3 0 1 は、取り外し可能な記録媒体とも接続可能である。そして、その記録媒体に記録されたデジタル画像データをデジタル署名データと共に入力する。

#### 【 0 0 4 1 】

作業用メモリ 3 0 2 は、デジタル画像データ等を一時的に保管し、デジタル画像データに対する伸長復号処理、後述のデジタル署名データの生成等に使  
用される。

#### 【 0 0 4 2 】

制御／演算部 3 0 3 は、ROM 3 0 5 に格納されている各種のプログラムに従って画像検証装置 2 0 全体の動作を制御する制御回路 3 1 0、デジタル画像データを伸長復号する(例えば、可変長復号し、逆量子化した後、逆 D C T 変換や逆ウェーブレット変換する)画像処理回路 3 1 1、後述のデジタル署名データの生成に必要なハッシュ関数演算やデジタル画像データを検証するための演算処理を行う演算回路 3 1 2、デジタル署名データの生成に必要な秘密情報を格納するメモリ 3 1 3、演算回路 3 1 2 に必要な乱数を生成する乱数発生回路 3 1 4 を含む。

#### 【 0 0 4 3 】

表示部 3 0 4 は、デジタル画像データを視覚的に表示する。又、表示部 3 0 4 は、そのデジタル画像データの検証結果をユーザに視覚的に表示する。尚、表示部 3 0 4 は、画像検証装置 2 0 と取り外し可能である。

#### 【 0 0 4 4 】

ROM 3 0 5 は、読み出し専用メモリであり、画像検証装置 2 0 全体の動作を制御するプログラム、画像処理を制御するプログラム、デジタル画像データの検証処理を制御するプログラムを格納している。操作部 3 0 6 は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部 3 0 3 に供給する。

#### 【 0 0 4 5 】

以下、第 1 ～第 6 の実施例では、図 2 の画像入力装置 1 0 が、デジタル画像

データと秘密情報とに基づいて、デジタル署名データを生成する手順について詳細に説明する。

【0046】

又、第7～第12の実施例では、図4の画像検証装置20が、画像入力装置10にて生成されたデジタル署名データに基づいて、デジタル画像データの正当性を検証する手順について詳細に説明する。

【0047】

(第1の実施例)

第1の実施例では、画像入力装置10が、機器固有の秘密情報Sとハッシュ関数とを用いてデジタル署名データhを生成する処理について説明する。具体的に説明すると、デジタル画像データPと秘密情報Sとを用いて予め定められた規則の演算を行い、ハッシュ関数を用いてその演算結果を演算し、その演算結果をデジタル画像データPに対するデジタル署名データhとする。

【0048】

図4は、第1の実施例の処理手順を説明するフローチャートである。以下、図4を用いて、デジタル署名データhを生成する手順を説明する。

【0049】

ステップS401において、操作部208は、ある被写体の光学像を撮像するか否かを指示する。撮像が指示された場合、制御／演算部206はステップS402を実行する。

【0050】

ステップS402において、撮像部201は、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのデジタル画像データPを生成する。その後、デジタル画像データPは、作業用メモリ202に格納される。

【0051】

ステップS403において、制御／演算部206（に含まれる画像処理回路211）は、作業用メモリ202に格納されたデジタル画像データPを1画面分の静止画像毎に高能率符号化する。1つの静止画像を高能率符号化する手法として例えば、DCT変換方式（具体的には、複数画素からなるブロック毎にDCT

変換、量子化及び可変長符号化する方式)、ウェーブレット変換方式(具体的には、複数画素からなるブロック毎にウェーブレット変換、量子化及び可変長符号化する方式)、J P E G方式、J B I G方式、MH方式、MMR方式、M P E G方式等を用いてもよい。尚、以下の実施例では、J P E G方式を用いて高能率符号化する場合について説明する。

## 【 0 0 5 2 】

ステップ S 4 0 4 において、制御／演算部 2 0 6 は、画像入力装置 1 0 の持つ秘密情報 S をメモリ 2 1 3 から読み出す。

## 【 0 0 5 3 】

ステップ S 4 0 5 において、制御／演算部 2 0 6 (に含まれる演算回路 2 1 2) は、上述の秘密情報 S と例えば J P E G 方式で高能率符号化されたデジタル画像データ P (以下、J P E G データと称する) とを用いて、予め定められた規則に基づく所定の演算を行う。

## 【 0 0 5 4 】

ここで、秘密情報 S と所定の演算処理とについて説明する。

## 【 0 0 5 5 】

まず、秘密情報 S とは、画像入力機器 1 0 の製造時に設定される機器固有の情報であり、一般に公開されることのない情報である。この秘密情報 S は、外部から容易に入手することができないように制御／演算部 2 0 6 の内部に組み込まれている。以下、第 1 の実施例では、上述の秘密情報 S を例えば “ 1 1 1 1 1 1 1 ” として説明する。

## 【 0 0 5 6 】

次に、上述の所定の演算処理について図 5 を用いて説明する。所定の演算処理とは、ある J P E G データ列から所定の位置のバイトデータを選択した後、そのバイトデータと秘密情報 S とをビット毎に排他的論理和演算し、そのバイトデータを別のデータに変換する処理のことである。ここで、所定の位置とは、J P E G データ列上の任意の位置に設定することができるが、第 1 の実施例では最上位のバイトデータを演算対象として説明する。

## 【 0 0 5 7 】

ステップ S 4 0 6 において、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）は、ハッシュ関数を用いて、所定の演算処理の施された J P E G データを演算し、デジタル署名データ  $h$  を生成する。

【0 0 5 8】

ここで、ハッシュ関数について説明する。

【0 0 5 9】

ハッシュ関数  $H$  とは、任意のビット長のデジタルデータ  $M$  から、一定のビット長となる出力  $h$  を生成する機能を持つ。この出力  $h$  は、ハッシュ値と呼ばれる（又は、デジタル署名、メッセージダイジェスト、デジタル指紋等とも呼ばれる）。通常、ハッシュ関数には、一方向性と衝突耐性が要求される。一方向性とは、ハッシュ値  $h$  が与えられた際に、 $h = H(M)$  となるデジタルデータ  $M$  の算出が計算量的に困難であることを示す。又、衝突耐性とは、デジタルデータ  $M$  が与えられた際に、 $H(M) = H(M')$  となるデジタルデータ  $M'$  ( $M \neq M'$ ) の算出および  $H(M) = H(M')$  且つ  $M \neq M'$  となるデジタルデータ  $M, M'$  の算出が計算量的に困難であることを示す。ハッシュ関数には、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、RIPEMD-160 等の方式が知られている。第 1 の実施例では、MD-5 方式を使用する例について説明する。尚、この MD-5 方式を用いて生成されるデジタル署名データのビット長は 128 ビットとなる。

【0 0 6 0】

ステップ S 4 0 7 において、記録再生部 2 0 3 は、制御／演算部 2 0 6 にて生成されたデジタル署名データとそれに対応するデジタル画像データとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0 0 6 1】

尚、図 4 に示す一連の処理手順を制御するプログラムは、ROM 2 0 7 に格納されている。このプログラムは、制御／演算部 2 0 6（に含まれる制御回路 2 1 0）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像  $P$  を撮像する毎に、それに対応したデジタル署名データ  $h$  を生成す

ることができる。

【 0 0 6 2 】

以上説明したように第 1 の実施例では、高能率符号化されたデジタル画像データ P と画像入力装置 1 0 に固有の秘密情報 S とを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した結果が、デジタル署名データ h となる。このように構成することによって、第 1 の実施例では、安全性も信頼性も高いデジタル署名データ h を、従来のシステムに比べて非常に簡単な構成によって実現することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【 0 0 6 3 】

この結果、秘密情報 S と所定の演算とを知らなければ、デジタル画像データ P に対応するデジタル署名データ h を不正に作り出すことはできないため、デジタル署名データ h に基づいてデジタル画像データ P の正当性を安全に検証することができる。又、一方向性関数の性質により、デジタル署名データ h から元のデータ（即ち、秘密情報 S を用いて所定の演算を行なったデジタル画像データ P）を知ることできないため、デジタル署名データ h からデジタル画像データ P の正当性を安全に検証することができる。

【 0 0 6 4 】

尚、第 1 の実施例では、秘密情報 S を画像入力装置 1 0 の製造時に設定された情報としたがそれに限るものではない。画像検証装置 2 0 の秘密情報と共有できるものであれば、乱数発生回路 2 1 4 が所定のアルゴリズムに基づいて生成したビット列でもよい。

【 0 0 6 5 】

又、第 1 の実施例では、上述の所定の演算処理の一例として、J P E G データのバイトデータと秘密情報とを排他的論理和演算する構成について説明したがそれに限るものではない。秘密情報 S を、高能率符号化されたデジタル画像データ P の一部に付加、合成、あるいは多重する処理で且つ逆演算可能な処理であれば、いかなる演算処理であってもよい。

【 0 0 6 6 】

又、第 1 の実施例では、デジタル画像データ P とデジタル署名データ h とを同じタイミングで生成する手順について説明したがそれに限るものではない。デジタル画像データ P を画像入力装置 1 0 から外部へ出力する前に必ずデジタル署名データ h を生成する構成であれば、デジタル署名データ h はどのタイミングで生成してもよい。例えば、デジタル画像データ P を外部インタフェース 2 0 5 を介して外部に出力する場合には、一度記録媒体に格納した後、そのデジタル画像データ P を外部へ出力する前に、デジタル署名データ h を生成するようにしてもよい。但し、デジタル画像データ P を取り外し可能な記録媒体に記憶する場合には、上述の手順でデジタル署名データ h を生成する。

## 【 0 0 6 7 】

## (第 2 の実施例)

第 2 の実施例では、第 1 の実施例に比べてより安全性の高いデジタル署名データ h を生成する手順について詳細に説明する。

## 【 0 0 6 8 】

図 6 は、第 2 の実施例の処理手順を説明するフローチャートである。以下、図 6 を用いて、デジタル署名データ h を生成する手順を説明する。

## 【 0 0 6 9 】

ステップ S 6 0 1 ～ S 6 0 3 の処理は、上述の第 1 の実施例のステップ S 4 0 1 ～ S 4 0 3 と同様の処理としてその説明を省略する。

ステップ S 6 0 4 において、制御／演算部 2 0 6 ( に含まれる乱数発生回路 2 1 4 ) は、所定の情報 ( 例えば、高能率符号化されたデジタル画像データ P のデータ量 ) を基にして、ビット長 m の乱数 R を生成する。この乱数 R が第 2 の実施例の秘密情報 S である。

## 【 0 0 7 0 】

次のステップ S 6 0 5 ～ S 6 0 6 では、第 2 の実施例における所定の演算を説明する。

## 【 0 0 7 1 】

ステップ S 6 0 5 において、制御／演算部 2 0 6 ( に含まれる演算回路 2 1 2 ) は、図 7 に示すように、1 画像分の J P E G データを所定の大きさ ( 例えば 1

28ビット長)のブロック $D_i$  ( $i = 1, 2, 3 \dots n$ )に分割する。ここで、 $D_1$ を最上位ブロックとする。J P E Gデータの総量が128の倍数にならない場合、128の倍数となるようにパディングする。例えば、図7に示すように、最後のブロックに“000...000”を付加する。

#### 【0072】

ステップS606において、制御／演算部206（に含まれる演算回路212）は、上述の乱数 $R$ と上述の $n$ 個のブロックとを用いて以下に示す手順の演算を行う。

#### 【0073】

まず、制御／演算部206は、図8に示すように、乱数 $R$ のビット数 $m$ を $n$ ビット（図7に示すブロック $D_i$ の個数 $n$ と同じ）とする。例えば、 $m \geq n$ の場合、最上位ビットから $n$ ビットまでのビット列を有効とし、それ以外のビット列を切り捨てる。又、 $m < n$ の場合、不足分のデータとして“111...111”を付加する。

#### 【0074】

次に、制御／演算部206は、図9に示すように、各ブロック $D_1 \sim D_n$ と各乱数 $R_1 \sim R_n$ とを用いて所定の演算を行う。具体的に説明すると、乱数 $R$ のビット $R_i$ とブロック $D_i$ の最下位ビットとの間で排他的論理和演算を行い、その演算を $i = 1 \sim n$ まで繰り返す。

#### 【0075】

ここで、ステップS606の演算は、乱数 $R_i$ とブロック $D_i$ の最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロック $D_i$ の一部に秘密情報（ビット長 $m$ の乱数 $R$ の一部）を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

#### 【0076】

ステップS607において、制御／演算部206（に含まれる演算回路212）は、ステップS606の出力をハッシュ関数で演算し、デジタル署名データ $h$ を生成する。尚、第2の実施例では、第1の実施例と同様に、MD-5方式のハッシュ関数を用いる。従って、デジタル署名データ $h$ のビット長は、128

ビットとなる。

【 0 0 7 7 】

ステップ S 6 0 7 の演算処理の一例について詳細に説明する。

【 0 0 7 8 】

まず、制御／演算部 2 0 6 は、ステップ S 6 0 6 の出力から 1 つまたは複数個のブロック D を選択する。その後、制御／演算部 2 0 6 は、選択されたブロックをハッシュ関数で演算し、デジタル署名データ h を生成する。

【 0 0 7 9 】

また、ステップ S 6 0 5 ～ S 6 0 7 の演算処理の他の例について、図 1 0 ～ 1 2 を用いて詳細に説明する。

【 0 0 8 0 】

制御／演算部 2 0 6 は、後述する 3 つの動作モードの何れか 1 つ又はこれらの組み合わせることによりハッシュ値を求める。特に、第 1 のモードや第 3 のモードでは、あるブロック（1 ブロックは、k ビット）の演算結果を用いて他のブロックのハッシュ値を求めるため、より安全性の高いデジタル署名データ h を生成することができる。又、前のブロックの演算結果が、次のブロックの演算結果に反映されるため、ブロック毎に J P E G データの正当性を検証することもできる。

【 0 0 8 1 】

①第 1 のモード

第 1 のモードについて図 1 0 を用いて説明する。図 1 0 は、制御／演算部 2 0 6 の構成の一部を示す図である。

【 0 0 8 2 】

図 1 0 において、演算回路 2 1 2 は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路 1 0 0 1 と、ハッシュ関数回路 1 0 0 1 の出力 h の一部（K ビット）を記憶するレジスタ 1 0 0 2 と、J P E G データを K ビットのブロックに分割する演算回路 1 0 0 3 と、演算回路 1 0 0 3 の出力とレジスタ 1 0 0 2 の出力とを排他的論理和演算する演算回路 1 0 0 4 とから構成される。

【 0 0 8 3 】

ハッシュ関数回路 1 0 0 1 の出力である 1 2 8 ビットのハッシュ値  $h$  の一部 (  $K$  ビット ) は、レジスタ 1 0 0 2 に入力される。レジスタ 1 0 0 2 には、例えば、ハッシュ値  $h$  の上位 6 4 ビットが一時的に格納される。

【 0 0 8 4 】

レジスタ 1 0 0 2 に格納された  $K$  ビットは、1 ブロックの J P E G データと排他的論理和演算され、その演算結果はハッシュ関数回路 1 0 0 1 に供給される。

【 0 0 8 5 】

上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がデジタル署名データとして出力される。

【 0 0 8 6 】

ここで、最初の演算では、レジスタ 1 0 0 2 に初期値を格納しておく必要がある。その初期値は、例えば図 1 3 に示すように、乱数  $R$  の下位  $K$  ビットを用いることができる。

【 0 0 8 7 】

尚、ブロック  $D_i$  の大きさが 6 4 の倍数とならない場合には、例えば後述の第 3 のモードと組合せて余りのビット列を演算するように構成してもよい。

【 0 0 8 8 】

## ②第 2 のモード

第 2 のモードについて図 1 1 を用いて説明する。図 1 1 は、制御／演算部 2 0 6 の構成の一部を示す図である。

【 0 0 8 9 】

図 1 1 において、演算回路 2 1 2 は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路 1 1 0 1 と、ハッシュ関数回路 1 1 0 1 に必要な入力値を供給するレジスタ 1 1 0 2 と、ハッシュ関数回路 1 1 0 1 の出力  $h$  の一部 (  $K$  ビット ) を出力するセレクタ 1 1 0 3 と、J P E G データを  $K$  ビットのブロックに分割する演算回路 1 1 0 4 と、演算回路 1 1 0 4 の出力とセレクタ 1 1 0 3 の出力とを排他的論理和演算する演算回路 1 1 0 5 とから構成される。

【 0 0 9 0 】

ハッシュ関数回路 1 1 0 1 は、乱数発生回路 2 1 4 にて生成された秘密情報（即ち、乱数 R）を初期値とするレジスタ 1 1 0 2 の値をハッシュ関数で演算する。

#### 【 0 0 9 1 】

ハッシュ関数回路 1 1 0 1 の出力である 1 2 8 ビットのハッシュ値 h は、セクタ 1 1 0 3 に入力される。セクタ 1 1 0 3 は、1 2 8 ビットのハッシュ値 h の内、例えば下位 K ビットを出力する。この K ビットは、次にハッシュ関数演算されるデータとしてレジスタ 1 1 0 2 に格納される。

#### 【 0 0 9 2 】

上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がデジタル署名データとして出力される。

#### 【 0 0 9 3 】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図 1 3 に示すように、上述の乱数 R の下位 K ビットを用いることができる。

#### 【 0 0 9 4 】

##### ③第 3 のモード

第 3 のモードについて図 1 2 を用いて説明する。図 1 2 は、制御／演算部 2 0 6 の構成の一部を示す図である。

#### 【 0 0 9 5 】

図 1 2 において、演算回路 2 1 2 は、所定のビット単位でハッシュ関数演算を行うハッシュ関数回路 1 2 0 1 と、ハッシュ関数回路 1 2 0 1 に必要な入力値を供給するレジスタ 1 2 0 2 と、ハッシュ関数回路 1 2 0 1 の出力 h の一部（K ビット）を出力するセクタ 1 2 0 3 と、P E G データを K ビットのブロックに分割する演算回路 1 2 0 4 と、演算回路 1 2 0 4 の出力とセクタ 1 2 0 3 の出力とを排他的論理和演算する演算回路 1 2 0 5 とから構成される。

#### 【 0 0 9 6 】

ハッシュ関数回路 1 2 0 1 は、乱数発生回路 2 1 4 にて生成された秘密情報を初期値とするレジスタ 1 2 0 2 の値を順次ハッシュ関数演算する。

## 【 0 0 9 7 】

ハッシュ関数回路 1 2 0 1 の出力である 1 2 8 ビットのハッシュ値  $h$  は、セクタ 1 2 0 3 に入力される。セクタ 1 2 0 3 は、1 2 8 ビットのハッシュ値  $h$  の内、例えば下位  $K$  ビットを出力する。この  $K$  ビットは、1 ブロックの J P E G データと排他的論理和演算され、その演算結果の一部は再びレジスタ 1 2 0 2 に格納される。

## 【 0 0 9 8 】

上述の演算は、所定のブロックに達するまで、各ブロックに対して繰り返される。そして、その所定のブロックから求めたハッシュ値がデジタル署名データとして出力される。

## 【 0 0 9 9 】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図 1 3 に示すように、上述の乱数  $R$  の下位  $K$  ビットを用いることができる。

## 【 0 1 0 0 】

ステップ S 6 0 8 において、記録再生部 2 0 3 は、制御／演算部 2 0 6 にて生成されたデジタル署名データ  $h$  とそれに対応するデジタル画像データ  $P$  とを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

## 【 0 1 0 1 】

尚、図 6 に示す一連の処理手順を制御するプログラムは、ROM 2 0 7 に格納されている。このプログラムは、制御／演算部 2 0 6 （に含まれる制御回路 2 1 0）によって読み出され、ユーザの撮像指示毎に起動される。

## 【 0 1 0 2 】

以上のように第 2 の実施例では、ある長さの乱数  $R$  から生成された秘密情報  $S$  と高能率符号化されたデジタル画像データ  $P$  とを用いて所定の演算を行い、その演算結果をハッシュ関数で演算してデジタル署名データ  $h$  を生成する。このように構成することによって、第 2 の実施例では、従来のシステムに比べて安全性も信頼性も高いデジタル署名データ  $h$  を簡単な構成によって実現することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化

することもできる。

【0103】

又、第2の実施例では、ハッシュ関数演算を上述の動作モードの1つまたは複数を組み合わせて実現することにより、第1の実施例に比べてより安全性の高いデジタル署名データ生成アルゴリズムを提供することができる。

【0104】

更に、第2の実施例では、第1の実施例と同様に、デジタル署名データhを用いて、デジタル画像データPがどの画像入力装置にて撮像されたかを特定することもできる。

【0105】

(第3の実施例)

第1、第2の実施例では、ハッシュ関数を用いてデジタル署名データhを生成する手順について説明した。

【0106】

これに対して、第3の実施例では、ハッシュ関数ではなく、共通鍵暗号を用いてデジタル署名データhを生成する手順について詳細に説明する。

【0107】

図14は、第3の実施例の処理手順を説明するフローチャートである。以下、図14を用いて、デジタル署名データhを生成する手順を説明する。

【0108】

ステップS1401～S1403の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0109】

ステップS1404において、制御／演算部206は、画像入力装置10の持つ固有の秘密情報Sをメモリ213から読み出す。第3の実施例では、“1111…1111”（128ビット）を秘密情報Sとして説明する。

【0110】

ステップS1405において、制御／演算部206（に含まれる演算回路212）は、作業用メモリ202に保持されたJPGデータを共通鍵暗号方式に基

づいて暗号化する。ここで、J P E G データを共通鍵暗号化する暗号鍵は、秘密情報 S から生成する。

#### 【0 1 1 1】

共通鍵暗号方式には現在様々なものが提案されているが、第 3 の実施例では D E S 方式を用いる。D E S 方式を使用する場合、暗号鍵のビット長は 5 6 ビットであるので、秘密情報 S の上位 5 6 ビットを暗号鍵とする（図 1 5 参照）。ここで、この暗号鍵のビット長は、使用する共通鍵暗号方式の種類によって異なるものである。従って、FEAL-nX, MITSY, IDEA を使用する場合、暗号鍵は 1 2 8 ビットであるので、秘密情報 S の上位 1 2 8 ビットを暗号鍵とする。又、FEAL-n, MULTI 2 を使用する場合、暗号鍵は 6 4 ビットであるので、秘密情報 S の上位 6 4 ビットを暗号鍵とする。

#### 【0 1 1 2】

ステップ S 1 4 0 5 における共通鍵暗号化処理について詳細に説明する。

#### 【0 1 1 3】

制御／演算部 2 0 6 は、後述する 3 つの動作モード（即ち、C B C モード、C F B モード、O F B モード）の何れか 1 つ又はこれらの組み合わせにより、J P E G データを暗号化する。何れの動作モードにおいても、入力データを攪乱しながら暗号化することができるため、より安全性の高い暗号化処理を実現できる。

#### 【0 1 1 4】

##### ① C B C (Cipher Block Chaining) モード

C B C モードを図 1 6 を用いて説明する。図 1 6 は、制御／演算部 2 0 6 の一部（即ち、演算回路 2 1 2）を示す図である。

#### 【0 1 1 5】

図 1 6 において、演算回路 2 1 2 は、6 4 ビット単位で暗号化を行う暗号化回路 1 6 0 1 と、暗号化回路 1 6 0 1 の出力を一時的に保持するレジスタ 1 6 0 2 と、J P E G データとレジスタ 1 6 0 2 の出力とを排他的論理和演算する演算回路 1 6 0 3 とから構成される。

#### 【0 1 1 6】

暗号化回路 1 6 0 1 は、6 4 ビットからなるブロック毎に、J P E G データを

暗号化する。暗号化回路 1 6 0 1 の出力は、レジスタ 1 6 0 2 に一時的に格納される。レジスタ 1 6 0 2 に格納された 6 4 ビットのデータは、次のブロックと排他的論理和演算され、その演算結果は暗号化回路 1 6 0 1 に供給される。最終的に、全てのブロックを暗号化した結果が暗号データとして出力される。この暗号データの一部が、ディジタル署名データ h となる。

## 【 0 1 1 7 】

ここで、最初のブロックの暗号化では、レジスタ 1 6 0 2 に初期値を格納しておく必要がある。その初期値は、例えば、秘密情報 S の下位 6 4 ビットを用いる（図 1 5 参照）。

## 【 0 1 1 8 】

尚、ブロックの大きさが 6 4 の倍数とならない場合には、例えば後述の O F B モードと組合せて余りのビット列を暗号化するように構成してもよい。

## 【 0 1 1 9 】

## ② O F B (Output Feedback) モード

O F B モードについて図 1 7 を用いて説明する。図 1 7 は、制御／演算部 2 0 6 の一部（即ち、演算回路 2 1 2）を示す図である。

## 【 0 1 2 0 】

図 1 7 において、演算回路 2 1 2 は、6 4 ビット単位で暗号化を行う暗号化回路 1 7 0 1 と、暗号化回路 1 7 0 1 に必要な入力値を供給するレジスタ 1 7 0 2 と、暗号化回路 1 7 0 1 の出力を選択的に出力するセレクタ 1 7 0 3 と、J P E G データとセレクタ 1 7 0 3 の出力とを排他的論理和演算する演算回路 1 7 0 4 とから構成される。

## 【 0 1 2 1 】

暗号化回路 1 7 0 1 は、レジスタ 1 7 0 2 に格納された 6 4 ビットのデータを暗号化する。暗号化回路 1 7 0 1 の出力は、セレクタ 1 7 0 3 に入力される。セレクタ 1 7 0 3 は、例えば下位 K ビットを出力する。この K ビットは、次に暗号化されるデータとしてレジスタ 1 7 0 2 に格納される。セレクタ 1 7 0 3 から出力された K ビットは、J P E G データの各ブロック（1 ブロックは、K ビット）と排他的論理和演算され、その結果が暗号データとなる。この暗号データの一部

が、デジタル署名データ h となる。

【 0 1 2 2 】

尚、最初の暗号化に必要な初期値は、例えば、秘密情報 S の下位 6 4 ビットを用いる（図 1 5 参照）。

【 0 1 2 3 】

③ C F B (Cipher Feedback) モード

C F B モードについて図 1 8 を用いて説明する。図 1 8 は、制御／演算部 2 0 6 の一部（即ち、演算回路 2 1 2）を示す図である。

【 0 1 2 4 】

図 1 8 において、演算回路 2 1 2 は、6 4 ビット単位で暗号化を行う暗号化回路 1 8 0 1 と、暗号化回路 1 8 0 1 に必要な入力値を供給するレジスタ 1 8 0 2 と、暗号化回路 1 8 0 1 の出力を選択的に出力するセレクタ 1 8 0 3 と、J P E G データとセレクタ 1 8 0 3 の出力とを排他的論理和演算する演算回路 1 8 0 4 とから構成される。

【 0 1 2 5 】

暗号化回路 1 8 0 1 は、レジスタ 1 8 0 2 に格納された 6 4 ビットのデータを暗号化する。暗号化回路 1 8 0 1 の出力は、セレクタ 1 8 0 3 に入力される。セレクタ 1 8 0 3 は、例えば下位 K ビットを出力する。セレクタ 1 8 0 3 から出力された K ビットは、1 ブロック（K ビット）の J P E G データと排他的論理和演算され、その結果は再びレジスタ 1 8 0 2 に格納される。最終的に、全てのブロックを処理した結果が暗号データとして出力される。この暗号データの一部が、デジタル署名データ h となる。

【 0 1 2 6 】

尚、最初の暗号化に必要な初期値は、例えば、秘密情報 S の下位 6 4 ビットを用いる（図 1 5 参照）。

【 0 1 2 7 】

ステップ S 1 4 0 6 において、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）は、ステップ S 1 4 0 5 にて生成された暗号データから特定のビット列をデジタル署名データとして抽出する。例えば、上述の暗号データの下位 1 2 8 ビ

ットをデジタル署名データとする。

【0128】

ステップS1407において、記録再生部203は、制御／演算部206（に含まれる演算回路212）にて生成されたデジタル署名データhとそれに対応するデジタル画像データPとを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【0129】

尚、図14に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。

【0130】

以上のように第3の実施例では、秘密情報Sの一部から生成した暗号鍵と高能率符号化されたデジタル画像データPとを用いて共通鍵暗号方式による暗号化を行い、暗号化されたデータからデジタル署名データhを生成する。このように構成することにより、第3の実施例では、第1、第2の実施例に比べて安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0131】

又、第3の実施例では、デジタル署名データhを用いて、デジタル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【0132】

尚、第3の実施例では、秘密情報Sを“1111…1111”（128ビット）としたがこれに限るものではない。例えば、乱数発生回路214が所定のアルゴリズムに基づいて発生させた乱数とすることも可能である。但し、この秘密情報Sは画像検証装置20と共有される。

【0133】

（第4の実施例）

第3の実施例では、ハッシュ関数ではなく共通鍵暗号を用いてデジタル署名

データ  $h$  を生成する手順について説明した。

【 0 1 3 4 】

これに対して、第 4 の実施例では、所定の演算（例えば、ビット挿入を含む逆演算可能な演算）を行い、その演算結果を共通鍵暗号方式で暗号化した後、暗号化されたデータからデジタル署名データ  $h$  を生成する手順について説明する。

【 0 1 3 5 】

図 1 9 は、第 4 の実施例の処理手順を説明するフローチャートである。以下、図 1 9 を用いて、デジタル署名データ  $h$  を生成する手順を説明する。

【 0 1 3 6 】

ステップ S 1 9 0 1 ～ S 1 9 0 3 の処理は、上述の第 1 の実施例のステップ S 4 0 1 ～ S 4 0 3 と同様の処理としてその説明を省略する。

【 0 1 3 7 】

ステップ S 1 9 0 4 ～ S 1 9 0 6 の処理は、上述の第 2 の実施例のステップ S 6 0 4 ～ S 6 0 6 と同様の処理（即ち、秘密情報である乱数  $R$  のビット  $R_i$  と J P E G データのブロック  $D_i$  とを用いた排他的論理和演算）としてその説明を省略する。

【 0 1 3 8 】

ここで、ステップ S 1 9 0 6 の演算は、上述のステップ S 6 0 6 と同様に、乱数  $R_i$  とブロック  $D_i$  の最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロック  $D_i$  の少なくとも一部に秘密情報  $S$ （ビット長  $m$  の乱数  $R$ ）の一部を付加、合成、多重する処理で且つ逆演算可能な処理であれば、いかなる演算処理であってもよい。

【 0 1 3 9 】

ステップ S 1 9 0 7 において、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）は、ステップ S 1 9 0 6 の出力を共通鍵暗号方式に従って暗号化する。ここで、制御／演算部 2 0 6 は、第 3 の実施例と同様に、D E S 方式を利用するものとし、その暗号化に必要な暗号鍵は、ステップ S 1 9 0 4 で生成した秘密情報  $S$  の上位 5 6 ビットとする（図 2 0 参照）。

【 0 1 4 0 】

ステップ S 1 9 0 7 における暗号化処理について詳細に説明する。

【 0 1 4 1 】

制御／演算部 2 0 6 は、上述した 3 つの動作モード（即ち、CBC モード、CFB モード、OFB モード）の何れか 1 つ又はこれらの組み合わせ、乱数 R のビット  $R_i$  と JPEG データのブロック  $D_i$  とを排他的論理和演算した結果を、順次暗号化する。何れの動作モードにおいても、入力データを攪乱しながら暗号化することができるため、より安全性の高い暗号化を実現できる。

【 0 1 4 2 】

ステップ S 1 9 0 8 において、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）は、ステップ S 1 9 0 7 にて生成された暗号データから特定のビット列をデジタル署名データ  $h$  として抽出する。例えば、暗号データの下位 1 2 8 ビットをデジタル署名データ  $h$  とする。

【 0 1 4 3 】

ステップ S 1 9 0 9 において、記録再生部 2 0 3 は、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）にて生成されたデジタル署名データ  $h$  とそれに対応するデジタル画像データ  $P$  とを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

【 0 1 4 4 】

尚、図 1 9 に示す一連の処理手順を制御するプログラムは、ROM 2 0 7 に格納されている。このプログラムは、制御／演算部 2 0 6（に含まれる制御回路 2 1 0）によって読み出され、ユーザの撮像指示毎に起動される。

【 0 1 4 5 】

以上のように第 4 の実施例では、乱数 R から生成された秘密情報 S と高能率符号化されたデジタル画像データ  $P$  とを用いて所定の演算を行い、その演算結果を共通鍵暗号方式により暗号化し、暗号化されたデータからデジタル署名データ  $h$  を生成する。このように構成することにより、第 4 の実施例では、第 3 の実施例に比べて安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

## 【 0 1 4 6 】

又、第 4 の実施例では、デジタル署名データ  $h$  を用いて、あるデジタル画像データ  $P$  がどの画像入力装置にて撮像されたかを特定することもできる。

## 【 0 1 4 7 】

## (第 5 の実施例)

第 1 ～第 4 の実施例では、画像入力装置 1 0 に固有の秘密情報  $S$  に基づいて、デジタル署名データ  $h$  を生成する構成について説明した。このような構成により第 1 ～第 4 の実施例では、デジタル署名データ  $h$  を用いて、あるデジタル画像データ  $P$  がどの画像入力装置にて撮像されたものであるかを特定することができる。

## 【 0 1 4 8 】

これに対して、第 5 の実施例では、外部装置（例えば、IC カード等）を画像入力装置 1 0 に接続し、この外部装置に固有の秘密情報  $S$  に基づいて、デジタル署名データ  $h$  を生成する構成について説明する。外部機器の持つ秘密情報  $S$  は、例えば、画像入力装置 1 0 を識別するための ID 情報、画像入力装置 1 0 を使用するユーザを識別するための ID 情報とすることができる。このように構成することにより、第 5 の実施例では、デジタル署名データ  $h$  を用いて、デジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって撮像されたものであるかを特定することができる。

## 【 0 1 4 9 】

図 2 1 は、第 5 の実施例の処理手順を説明するフローチャートである。以下、図 2 1 を用いて、デジタル署名データ  $h$  を生成する手順を説明する。

## 【 0 1 5 0 】

ステップ S 2 1 0 1 において、画像入力装置 1 0 の制御/演算処理部 2 0 6 は、外部 I / F 部 2 0 5 に外部装置 4 0 が接続されているか否かを検出する。

## 【 0 1 5 1 】

ステップ S 2 1 0 2 において、画像入力装置 1 0 と外部装置 4 0 とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

## 【 0 1 5 2 】

図 2 2 を用いて、画像入力装置 1 0 と外部装置 4 0 との相互認証処理について説明する。

## 【 0 1 5 3 】

画像入力装置 1 0 は、乱数発生回路 2 1 4 を用いて認証用の乱数  $a$  を発生させ、その乱数  $a$  を外部 I / F 部 2 0 5 を介して外部装置 4 0 に送信する。

## 【 0 1 5 4 】

次に外部装置 4 0 の暗号化回路 4 3 は、認証用の暗号鍵を用いて乱数  $a$  を  $A$  に変換し、その暗号データ  $A$  を外部 I / F 部 4 1 を介して画像入力装置 1 0 へ送信する。

## 【 0 1 5 5 】

又、画像入力装置 1 0 の暗号化回路 2 2 0 1 は、乱数  $a$  を認証用の暗号鍵を用いて  $A'$  に変換する。比較回路 2 2 0 2 は、その暗号データ  $A'$  を外部装置 4 0 から送信された暗号データ  $A$  と比較し、それらが一致すれば外部装置 4 0 を認証する。

## 【 0 1 5 6 】

同様にして、外部装置 4 0 は、乱数発生回路 4 2 を用いて認証用の乱数  $b$  を発生させ、その乱数  $b$  を外部 I / F 部 2 0 5 を介して画像入力装置 1 0 に送信する。

## 【 0 1 5 7 】

次に画像入力装置 1 0 の暗号化回路 2 2 0 1 は、認証用の暗号鍵を用いて乱数  $b$  を  $B$  に変換し、その暗号データ  $B$  を外部 I / F 部 2 0 5 を介して外部装置 4 0 へ送信する。

## 【 0 1 5 8 】

又、外部装置 4 0 の暗号化回路 4 3 は、乱数  $b$  を認証用の暗号鍵を用いて  $B'$  に変換する。比較回路 4 4 は、その暗号データ  $B'$  を画像入力装置 1 0 から送信された暗号データ  $B$  と比較し、それらが一致すれば画像入力装置 1 0 を認証する。

## 【 0 1 5 9 】

双方が正常に認証された場合、外部装置 4 0 は、メモリ 4 5 に格納された秘密情報 S を外部 I / F 部 4 1 を介して画像入力装置 1 0 に送信する。

## 【 0 1 6 0 】

ステップ S 2 1 0 3 ~ S 2 1 0 5 の処理は、上述の第 1 の実施例のステップ S 4 0 1 ~ S 4 0 3 と同様の処理としてその説明を省略する。

## 【 0 1 6 1 】

ステップ S 2 1 0 6 において、制御 / 演算部 2 0 6 は、外部 I / F 部 2 0 5 を介して入力された秘密情報 S をメモリ 2 1 3 に格納する。

## 【 0 1 6 2 】

ステップ S 2 1 0 7 において、制御 / 演算部 2 0 6 （に含まれる演算回路 2 1 2）は、秘密情報 S と J P E G 方式で高能率符号化されたデジタル画像データ P （以下、J P E G データと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路 2 1 2 は、第 1 の実施例のステップ S 4 0 5 と同様の演算を行う。

## 【 0 1 6 3 】

ステップ S 2 1 0 8 において、制御 / 演算部 2 0 6 （に含まれる演算回路 2 1 2）は、ステップ S 2 1 0 7 の演算結果をハッシュ関数で演算し、その結果からデジタル署名データ h を生成する。ここで、演算回路 2 1 2 は、第 1 の実施例のステップ S 4 0 6 と同様の演算処理を行う。

## 【 0 1 6 4 】

ステップ S 2 1 0 9 において、記録再生部 2 0 3 は、制御 / 演算部 2 0 6 にて生成されたデジタル署名データ h とそれに対応するデジタル画像データ P とを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

## 【 0 1 6 5 】

尚、図 2 1 に示す一連の処理手順を制御するプログラムは、ROM 2 0 7 に格納されている。このプログラムは、制御 / 演算部 2 0 6 （に含まれる制御回路 2 1 0）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像を撮像する毎にその画像に対応したデジタル署名データ h を生成

することができる。

【0166】

以上のように第5の実施例では、高能率符号化されたデジタル画像データPと外部装置40の有する秘密情報Sとを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した後、その演算結果からデジタル署名データhを生成する。このように構成することにより、第5の実施例では、従来のシステムに比べて安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

【0167】

この結果、外部機器の秘密情報Sと所定の演算とを知らなければ、デジタル画像データPに対応するデジタル署名データhを不正に作り出すことはできないため、デジタル署名データhに基づいてデジタル画像データPの正当性を安全に検証することができる。又、一方向性関数の性質により、デジタル署名データhから元のデータ（即ち、秘密情報Sを用いて所定の演算を行なったデジタル画像データP）を知ることもしないため、デジタル署名データhからデジタル画像データPの正当性を安全に検証することができる。

【0168】

又、デジタル署名データhを用いて、デジタル画像データがどのユーザによって撮像されたかを特定することもできる。

【0169】

尚、第5の実施例では、デジタル署名データhを生成する手順を第1の実施例と同様の手順としたがそれに限るものではない。上述の第2～第4の実施例の何れも適用することができる。

【0170】

（第6の実施例）

第5の実施例では、画像入力装置10に外部装置40を接続し、この外部装置40の持つ固有の秘密情報に基づいてデジタル署名データを生成する構成について説明した。

## 【 0 1 7 1 】

これに対して、第 6 の実施例では、画像入力装置 1 0 を外部装置 4 0 に接続し、この外部装置 4 0 に固有の秘密情報 S 2 と画像入力装置 1 0 に固有の秘密情報 S 1 の双方に基づいて、デジタル署名データ h を生成する構成について説明する。このように構成することにより第 6 の実施例では、デジタル署名データ h を用いて、デジタル画像データ P がどの外部機器と接続されたどの画像入力装置によって撮像されたものか、或いはどのユーザが使用するどの画像入力装置によって撮像されたものであるかを特定することができる。

## 【 0 1 7 2 】

図 2 1 を用いて第 6 の実施例の処理手順を詳細に説明する。

## 【 0 1 7 3 】

ステップ S 2 1 0 1 において、画像入力装置 1 0 の制御/演算処理部 2 0 6 は、外部 I / F 部 2 0 5 に外部装置 4 0 が接続されているか否かを検出する。

## 【 0 1 7 4 】

ステップ S 2 1 0 2 において、画像入力装置 1 0 と外部装置 4 0 とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

## 【 0 1 7 5 】

ステップ S 2 1 0 3 ～ S 2 1 0 5 の処理は、上述の第 1 の実施例のステップ S 4 0 1 ～ S 4 0 3 と同様の処理としてその説明を省略する。

## 【 0 1 7 6 】

ステップ S 2 1 0 6 において、制御/演算部 2 0 6 は、画像入力装置 1 0 の持つ秘密情報 S 1 をメモリ 2 1 3 から読み出すと共に、外部装置 4 0 の持つ秘密情報 S 2 を外部 I / F 部 2 0 5 を介して入力する。そして、これらの秘密情報 S 1 , S 2 を結合させ、新しい秘密情報 S を生成する。

## 【 0 1 7 7 】

ここで、画像入力装置 1 0 の秘密情報 S 1 を例えば “ 1 1 1 1 ” とし、外部装置 4 0 の秘密情報 S 2 を例えば “ 0 0 0 0 ” とすると、新たに生成される秘密情報 S は、例えば “ 1 1 1 1 0 0 0 0 ” となる。尚、第 6 の実施例では、2 つの秘密情報を単に結合することにより新たな秘密情報 S を生成する場合について説明

したが、秘密情報 S から秘密情報 S 1, S 2 を抽出できる演算であれば、いかなる演算であってもよい。

## 【 0 1 7 8 】

ステップ S 2 1 0 7 において、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）は、秘密情報 S と J P E G 方式で高能率符号化されたデジタル画像データ P（以下、J P E G データと称する）とを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路 2 1 2 は、第 1 の実施例のステップ S 4 0 5 と同様の演算を行う。

## 【 0 1 7 9 】

ステップ S 2 1 0 8 において、制御／演算部 2 0 6（に含まれる演算回路 2 1 2）は、ステップ S 2 1 0 7 の演算結果をハッシュ関数で演算し、その結果からデジタル署名データ h を生成する。

## 【 0 1 8 0 】

ステップ S 2 1 0 9 において、記録再生部 2 0 3 は、制御／演算部 2 0 6 にて生成されたデジタル署名データ h とそれに対応するデジタル画像データ P とを、取り外し可能な記録媒体に記録したり、ネットワークを介して他の機器に出力したりする。

## 【 0 1 8 1 】

尚、図 2 1 に示す一連の処理手順を制御するプログラムは、ROM 2 0 7 に格納されている。このプログラムは、制御／演算部 2 0 6（に含まれる制御回路 2 1 0）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像を撮像する毎にその画像に対応したデジタル署名データを生成することができる。

## 【 0 1 8 2 】

以上説明したように、第 6 の実施例では、高能率符号化されたデジタル画像データ P と、画像入力装置 1 0 の秘密情報 S 1 と外部装置 4 0 の秘密情報 S 2 とから生成された秘密情報 S とを用いて所定の演算を行い、その演算結果をハッシュ関数で演算した後、その演算結果を用いてデジタル署名データ h を生成する。このように構成することにより、第 6 の実施例では、従来のシステムに比べて

安全性も信頼性も向上させたデジタル署名データを生成することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

## 【 0 1 8 3 】

又、デジタル署名データ h を用いて、デジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって使用された画像入力装置にて撮像されたものかを特定することもできる。

## 【 0 1 8 4 】

尚、第 6 の実施例では、デジタル署名データ h を生成する手順を第 1 の実施例と同様の手順としたがそれに限るものではない。上述の第 2 ～第 4 の実施例の何れも適用することができる。

## 【 0 1 8 5 】

## (第 7 の実施例)

第 7 の実施例では、第 1 の実施例の画像入力装置 1 0 が生成したデジタル署名データ h を用いて、デジタル画像データ P の正当性を確認する画像検証装置 2 0 について説明する。

## 【 0 1 8 6 】

図 2 3 は、第 7 の実施例の処理手順の一例を説明するフローチャートである。以下、図 2 3 を用いて、画像検証装置 2 0 がデジタル画像データ P を検証する手順を説明する。

## 【 0 1 8 7 】

ステップ S 2 3 0 1 において、外部 I / F 部 3 0 1 は、画像入力装置 1 0 が生成したデジタル画像データ P とそれに対応するデジタル署名データ h とを入力し、それらを画像検証装置 2 0 の作業用メモリ 3 0 2 に格納する。ここで、デジタル画像データ P は、例えば、J P E G 方式で高能率符号化されている（以下、デジタル画像データ P を単に J P E G データと称する）。

## 【 0 1 8 8 】

ステップ S 2 3 0 2 において、操作部 3 0 6 は、ユーザの操作入力に基づき、どの J P E G データの正当性を検証するか否かを選択する。検証が指示された場

合、制御／演算部 3 0 3 はステップ S 2 3 0 3 を実行する。

【 0 1 8 9 】

ステップ S 2 3 0 3 において、制御／演算部 3 0 3 は、メモリ 3 1 3 から秘密情報 S を読み出す。ここで、この秘密情報 S は、第 1 の実施例の画像入力装置 1 0 と本実施例の画像検証装置 2 0 との間で秘密に共有する情報である。従って、本実施例の秘密情報 S は、第 1 の実施例と同様に “ 1 1 1 1 1 1 1 ” である。尚、この秘密情報 S は、読み出し専用の記録媒体等の中に保存され、外部に出力できないように管理されている。

【 0 1 9 0 】

ステップ S 2 3 0 4 において、制御／演算部 3 0 3 （に含まれる演算回路 3 1 2）は、秘密情報 S と J P E G データとを用いて、第 1 の実施例のステップ S 4 0 5 と同様の演算を行う。つまり、J P E G データの最上位バイトと秘密情報 S とを、ビット毎に排他的論理和演算する。

【 0 1 9 1 】

ステップ S 2 3 0 5 において、制御／演算部 3 0 3 （に含まれる演算回路 3 1 2）は、ステップ S 2 3 0 4 の演算結果をハッシュ関数で演算する。ここでは、第 1 の実施例と同様のハッシュ関数を使用して、ステップ S 4 0 6 と同様の処理を行う。

【 0 1 9 2 】

ステップ S 2 3 0 6 において、制御／演算部 3 0 3 （に含まれる演算回路 3 1 2）は、ステップ S 2 3 0 5 の演算結果と選択された J P E G データのデジタル署名データ h とを比較する。比較の結果、これらのデータが一致した場合には、J P E G データを正当なものと判断し、一致しなかった場合には、J P E G データに何らかの不正な処理（即ち、J P E G データに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【 0 1 9 3 】

ステップ S 2 3 0 7 において、表示部 3 0 4 は、ステップ S 2 3 0 6 の比較結果が一致した場合、選択した J P E G データが正常で、不正な処理の施されていないことを示す表示画像或いはメッセージを表示する。又、この比較結果が一致

しなかった場合、不正な処理を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

## 【 0 1 9 4 】

尚、図 2 3 に示す一連の処理手順を制御するプログラムは、R O M 3 0 5 に格納されている。このプログラムは、制御／演算部 3 0 3 （に含まれる制御回路 3 1 2）によって読み出され、所望の画像の検証を指示する毎に起動する。

## 【 0 1 9 5 】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 3 1 0 は各処理回路を制御して該 J P E G データを廃棄する。

## 【 0 1 9 6 】

以上説明したように、第 7 の実施例では、第 1 の実施例の画像入力装置 1 0 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

## 【 0 1 9 7 】

## （第 8 の実施例）

第 8 の実施例では、第 2 の実施例の画像入力装置 1 0 が生成したデジタル署名データ h を用いて、デジタル画像データ P の正当性を確認する画像検証装置 2 0 について説明する。

## 【 0 1 9 8 】

図 2 4 は、第 8 の実施例の処理手順の一例を説明するフローチャートである。以下、図 2 4 を用いて、画像検証装置 2 0 がデジタル画像データ P を検証する手順を説明する。

## 【 0 1 9 9 】

ステップ S 2 4 0 1、S 2 4 0 2 の処理は、上述の第 7 の実施例のステップ S 2 3 0 1、S 2 3 0 2 と同様の処理としてその説明を省略する。

## 【 0 2 0 0 】

ステップ S 2 4 0 3 において、制御／演算部 3 0 3 （に含まれる乱数発生回路

）は、ビット長 $m$ の乱数 $R$ （即ち、秘密情報 $S$ ）を生成する。乱数 $R$ を生成するためのプログラムは、ROM 305に格納されている。このプログラムは、第2の実施例の画像入力装置10の保持するプログラムと同一であり、乱数 $R$ は、第2の実施例の乱数 $R$ と同一である。尚、このプログラム及び乱数 $R$ は、外部に出力できないように管理されている。

#### 【0201】

ステップS2404において、制御／演算部303（に含まれる演算回路312）は、図7に示すように、選択されたJPEGデータを128ビットのブロック $D_i$ （ $i = 1 \sim n$ ）に分割する。データ量が128ビットにならないブロックについては、“000…000”をパディングする。尚、ステップS2404の処理は、第2の実施例のステップS605と同様の処理である。

#### 【0202】

ステップS2405において、制御／演算部303（に含まれる演算回路312）は、乱数 $R$ と $n$ 個のブロックとを用いて、第2の実施例のステップS606と同様の演算を行う。つまり、乱数 $R$ のビット $R_i$ とブロック $D_i$ の最下位ビットとの間の排他的論理和演算を、 $i = 1 \sim n$ となるまで繰り返す。

#### 【0203】

ステップS2406において、制御／演算部303（に含まれる演算回路312）は、ステップS2405の演算結果に対してハッシュ関数演算を行う。ここでは、第2の実施例と同様のハッシュ関数を使用して、ステップS607と同様の処理を行う。

#### 【0204】

ステップS2407において、制御／演算部303（に含まれる演算回路312）は、ステップS2406の演算結果と選択されたJPEGデータのデジタル署名データ $h$ とを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、JPEGデータに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

#### 【0205】

ステップ S 2 4 0 8 において、表示部 3 0 4 は、ステップ S 2 4 0 7 の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

#### 【 0 2 0 6 】

尚、図 2 4 に示す一連の処理手順を制御するプログラムは、R O M 3 0 5 に格納されている。このプログラムは、制御／演算部 3 0 3（に含まれる制御回路 3 1 2）によって読み出され、所望の画像の検証を指示する毎に起動する。

#### 【 0 2 0 7 】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 3 1 0 は各処理回路を制御して該 J P E G データを廃棄する。

#### 【 0 2 0 8 】

以上説明したように、第 8 の実施例では、第 2 の実施例の画像入力装置 1 0 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

#### 【 0 2 0 9 】

##### （第 9 の実施例）

第 9 の実施例では、第 3 の実施例の画像入力装置 1 0 が生成したデジタル署名データ h を用いて、デジタル画像データ P の正当性を確認する画像検証装置 2 0 について説明する。

#### 【 0 2 1 0 】

図 2 5 は、第 9 の実施例の処理手順の一例を説明するフローチャートである。以下、図 2 5 を用いて、画像検証装置 2 0 がデジタル画像データ P を検証する手順を説明する。

#### 【 0 2 1 1 】

ステップ S 2 5 0 1、S 2 5 0 2 の処理は、上述の第 7 の実施例のステップ S 2 3 0 1、S 2 3 0 2 と同様の処理としてその説明を省略する。

#### 【 0 2 1 2 】

ステップ S 2 5 0 3 において、制御／演算部 3 0 3 は、メモリ 3 1 3 から秘密

情報 S を読み出す。ここで、この秘密情報 S は、第 3 の実施例の画像入力装置 1 0 と本実施例の画像検証装置 2 0 との間で共有する情報である。従って、本実施例の秘密情報 S は、第 3 の実施例と同様に “1 1 1 1 1 1 1 1” である。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部に出力できないように管理されている。

【 0 2 1 3 】

ステップ S 2 5 0 4 において、制御／演算部 3 0 3 （に含まれる演算回路 3 1 2）は、第 3 の実施例のステップ S 1 4 0 5 と同様に、選択された J P E G データを共通鍵暗号方式で暗号化する。

【 0 2 1 4 】

ステップ S 2 5 0 5 において、制御／演算部 3 0 3 （に含まれる演算回路 3 1 2）は、ステップ S 2 5 0 4 にて生成された暗号データから特定のビット列を抽出する。例えば、第 3 の実施例と同様に、上述の暗号データの下位 1 2 8 ビットを抽出する。

【 0 2 1 5 】

ステップ S 2 5 0 6 において、制御／演算部 3 0 3 （に含まれる演算回路 3 1 2）は、ステップ S 2 5 0 5 の抽出結果と選択された J P E G データのデジタル署名データ h とを比較する。比較の結果、これらのデータが一致した場合には、J P E G データを正当なものと判断し、一致しなかった場合には、J P E G データに何らかの不正な処理（即ち、J P E G データに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

【 0 2 1 6 】

ステップ S 2 5 0 7 において、表示部 3 0 4 は、ステップ S 2 5 0 6 の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

【 0 2 1 7 】

尚、図 2 5 に示す一連の処理手順を制御するプログラムは、R O M 3 0 5 に格納されている。このプログラムは、制御／演算部 3 0 3 （に含まれる制御回路 3 1 2）によって読み出され、所望の画像の検証を指示する毎に起動する。

## 【 0 2 1 8 】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 3 1 0 は各処理回路を制御して該 J P E G データを廃棄する。

## 【 0 2 1 9 】

以上説明したように、第 9 の実施例では、第 3 の実施例の画像入力装置 1 0 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

## 【 0 2 2 0 】

(第 1 0 の実施例)

第 1 0 の実施例では、第 4 の実施例の画像入力装置 1 0 が生成したデジタル署名データ h を用いて、デジタル画像データ P の正当性を確認する画像検証装置 2 0 について説明する。

## 【 0 2 2 1 】

図 2 6 は、第 1 0 の実施例の処理手順の一例を説明するフローチャートである。以下、図 2 6 を用いて、画像検証装置 2 0 がデジタル画像データ P を検証する手順を説明する。

## 【 0 2 2 2 】

ステップ S 2 6 0 1、S 2 6 0 2 の処理は、上述の第 7 の実施例のステップ S 2 3 0 1、S 2 3 0 2 と同様の処理としてその説明を省略する。

## 【 0 2 2 3 】

ステップ S 2 6 0 3 ～ S 2 6 0 5 の処理は、上述の第 8 の実施例のステップ S 2 4 0 3 ～ S 2 4 0 5 と同様の処理としてその説明を省略する。

## 【 0 2 2 4 】

ステップ S 2 6 0 6 において、制御／演算部 3 0 3 ( に含まれる演算回路 3 1 2 ) は、第 4 の実施例のステップ S 1 9 0 7 と同様に、選択された J P E G データを共通鍵暗号方式で暗号化する。

## 【 0 2 2 5 】

ステップ S 2 6 0 7 において、制御／演算部 3 0 3 ( に含まれる演算回路 3 1

2) は、ステップ S 2 6 0 6 にて生成された暗号データから特定のビット列を抽出する。例えば、第 3 の実施例と同様に、上述の暗号データの下位 1 2 8 ビットを抽出する。

#### 【 0 2 2 6 】

ステップ S 2 6 0 8 において、制御／演算部 3 0 3 ( に含まれる演算回路 3 1 2 ) は、ステップ S 2 6 0 7 の抽出結果と選択された J P E G データのデジタル署名データ h とを比較する。比較の結果、これらのデータが一致した場合には、J P E G データを正当なものと判断し、一致しなかった場合には、J P E G データに何らかの不正な処理 ( 即ち、J P E G データに対する修正、改竄、偽造、合成等の改変処理 ) が行われたものと判断する。

#### 【 0 2 2 7 】

ステップ S 2 6 0 9 において、表示部 3 0 4 は、ステップ S 2 6 0 8 の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

#### 【 0 2 2 8 】

尚、図 2 6 に示す一連の処理手順を制御するプログラムは、ROM 3 0 5 に格納されている。このプログラムは、制御／演算部 3 0 3 ( に含まれる制御回路 3 1 2 ) によって読み出され、所望の画像の検証を指示する毎に起動する。

#### 【 0 2 2 9 】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 3 1 0 は各処理回路を制御して該 J P E G データを廃棄する。

#### 【 0 2 3 0 】

以上説明したように、第 1 0 の実施例では、第 4 の実施例の画像入力装置 1 0 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。

#### 【 0 2 3 1 】

##### ( 第 1 1 の実施例 )

第 1 1 の実施例では、第 5 の実施例の画像入力装置 1 0 が生成したデジタル

署名データhを用いて、デジタル画像データPの正当性を確認する画像検証装置20について説明する。

【0232】

図27は、第11の実施例の処理手順の一例を説明するフローチャートである。以下、図27を用いて、画像検証装置20がデジタル画像データPを検証する手順を説明する。

【0233】

ステップS2701において、画像検証装置20の制御/演算処理部303は、外部I/F部301に外部装置40が接続されているか否かを検出する。

【0234】

ステップS2702において、画像検証装置20と外部装置40とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【0235】

ステップS2703、S2704の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0236】

ステップS2705において、制御/演算部303は、外部I/F部301を介して入力された外部装置40に固有の秘密情報Sをメモリ313に格納し、管理する。

【0237】

ステップS2706において、制御/演算部303（に含まれる演算回路312）は、秘密情報SとJPEGデータとを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路312は、第7の実施例のステップS2304と同様の演算を行う。

【0238】

ステップS2707において、制御/演算部303（に含まれる演算回路312）は、ステップS2706の演算結果をハッシュ関数で演算する。ここで、演算回路312は、第7の実施例のステップS2305と同様の演算を行う。

【0239】

ステップ S 2 7 0 8 において、制御／演算部 3 0 3（に含まれる演算回路 3 1 2）は、ステップ S 2 7 0 7 の演算結果と選択された J P E G データのデジタル署名データ h とを比較する。比較の結果、これらのデータが一致した場合には、J P E G データを正当なものと判断し、一致しなかった場合には、J P E G データに何らかの不正な処理（即ち、J P E G データに対する修正、改竄、偽造、合成等の改変処理）が行われたものと判断する。

## 【 0 2 4 0 】

ステップ S 2 7 0 9 において、表示部 3 0 4 は、ステップ S 2 7 0 8 の比較結果を画像或いはメッセージで表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

## 【 0 2 4 1 】

尚、図 2 7 に示す一連の処理手順を制御するプログラムは、R O M 3 0 5 に格納されている。このプログラムは、制御／演算部 3 0 3（に含まれる制御回路 3 1 2）によって読み出され、所望の画像の検証を指示する毎に起動する。

## 【 0 2 4 2 】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 3 1 0 は各処理回路を制御して該 J P E G データを廃棄する。

## 【 0 2 4 3 】

以上説明したように、第 1 1 の実施例では、第 5 の実施例の画像入力装置 1 0 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。更に、デジタル署名データ h を用いて、デジタル画像データがどの外部機器によって撮像されたものか、或いはどのユーザにて撮像されたものかを特定することもできる。

## 【 0 2 4 4 】

## （第 1 2 の実施例）

第 1 2 の実施例では、第 6 の実施例の画像入力装置 1 0 が生成したデジタル署名データ h を用いて、デジタル画像データ P の正当性を確認する画像検証装

置 2 0 について説明する。

【 0 2 4 5 】

図 2 7 を用いて、第 1 2 の実施例の処理手順の一例を説明する。

【 0 2 4 6 】

ステップ S 2 7 0 1 ～ S 2 7 0 4 の処理は、上述の第 1 1 の実施例と同様の処理としてその説明を省略する。

【 0 2 4 7 】

ステップ S 2 7 0 5 において、制御／演算部 3 0 3 は、画像入力装置 1 0 と供給する秘密情報 S 1 をメモリ 3 1 3 から読み出し、外部装置 4 0 に固有の秘密情報 S 2 を外部 I / F 部 3 0 1 を介して入力する。そして、第 6 の実施例と同様に、これらの秘密情報 S 1 , S 2 を結合し、新しい秘密情報 S を生成する。

【 0 2 4 8 】

ステップ S 2 7 0 6 において、制御／演算部 3 0 3 ( に含まれる演算回路 3 1 2 ) は、秘密情報 S と J P E G データとを用いて、予め定められた規則に基づく所定の演算を行う。ここで、演算回路 3 1 2 は、第 7 の実施例のステップ S 2 3 0 4 と同様の演算処理を行う。

【 0 2 4 9 】

ステップ S 2 7 0 7 において、制御／演算部 3 0 3 ( に含まれる演算回路 3 1 2 ) は、ステップ S 2 7 0 6 の演算結果をハッシュ関数で演算する。ここで、演算回路 3 1 2 は、第 7 の実施例のステップ S 2 3 0 5 と同様の演算処理を行う。

【 0 2 5 0 】

ステップ S 2 7 0 8 において、制御／演算部 3 0 3 ( に含まれる演算回路 3 1 2 ) は、ステップ S 2 7 0 7 の演算結果と選択された J P E G データのデジタル署名データ h とを比較する。比較の結果、これらのデータが一致した場合には、J P E G データを正当なものと判断し、一致しなかった場合には、J P E G データに何らかの不正な処理 ( 即ち、J P E G データに対する修正、改竄、偽造、合成等の改変処理 ) が行われたものと判断する。

【 0 2 5 1 】

ステップ S 2 7 0 9 において、表示部 3 0 4 は、ステップ S 2 7 0 8 の比較結

果を画像或いはメッセージで表示する。これにより、ユーザは、選択した J P E G データの正当性を視覚的に分かり易く認識することができる。

## 【 0 2 5 2 】

尚、図 2 7 に示す一連の処理手順を制御するプログラムは、ROM 3 0 5 に格納されている。このプログラムは、制御／演算部 3 0 3 （に含まれる制御回路 3 1 2）によって読み出され、所望の画像の検証を指示する毎に起動する。

## 【 0 2 5 3 】

以上の手順により、選択された J P E G データの正当性が確認されなかった場合、制御回路 3 1 0 は各処理回路を制御して該 J P E G データを廃棄する。

## 【 0 2 5 4 】

以上説明したように、第 1 2 の実施例では、第 6 の実施例の画像入力装置 1 0 にて撮像され、高能率符号化されたデジタル画像データ P の正当性を、従来のシステムに比べて簡単な構成で認識することができる。又、従来のシステムに比べて安価に構成することも、処理速度を高速化することもできる。更に、上述のデジタル署名データ h を用いて、デジタル画像データがどの外部機器と接続された画像入力装置によって撮像されたものか、或いはどのユーザによって使用された画像入力装置にて撮像されたものかを特定することもできる。

## 【 0 2 5 5 】

尚、本発明はその精神、又は主要な特徴から逸脱することなく、他の様々な形で実施することができる。

## 【 0 2 5 6 】

例えば、第 1 ～第 6 の実施例では、画像入力装置 1 0 内においてデジタル署名データを生成したが、該デジタル署名データを画像入力装置 1 0 に接続された外部装置 4 0 にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、高能率符号化されたデジタル画像データ等を画像入力装置 1 0 から外部装置 4 0 に送信し、デジタル署名データを生成する。

## 【 0 2 5 7 】

又、第 1 ～第 6 の実施例では、デジタル署名データの生成に必要な演算処理

を画像入力装置 1 0 と外部装置 4 0 とに分散させ、各装置が共同してデジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、高能率符号化されたデジタル画像データ等の中で必要な部分のみを画像入力装置 1 0 から外部装置 4 0 に送信し、デジタル署名データを生成する。

## 【 0 2 5 8 】

又、第 7 ～ 第 1 2 の実施例では、画像検証装置 2 0 が外部入力されたデジタル画像データを用いてデジタル署名データを生成したが、該デジタル署名データを画像検証装置 2 0 に接続された外部装置 4 0 にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、外部入力されたデジタル画像データ等を画像検証装置 2 0 から外部装置 4 0 に送信し、デジタル署名データを生成する。

## 【 0 2 5 9 】

又、第 7 ～ 第 1 2 の実施例では、デジタル署名データの生成に必要な演算処理を画像検証装置 2 0 と外部装置 4 0 とに分散させ、各装置が共同してデジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、外部入力されたデジタル画像データ等の中で必要な部分のみを画像検証装置 2 0 から外部装置 4 0 に送信し、デジタル署名データを生成する。

## 【 0 2 6 0 】

又、第 7 ～ 第 1 2 の実施例では、図 2 3 ～ 図 2 7 に示す一連の処理手順を制御するプログラムは、所望の画像の検証を指示する毎に起動する構成として説明したが、所望の画像を外部入力することに自動的に起動するように構成してもよい。

## 【 0 2 6 1 】

従って、前述の各実施例ではあらゆる点で単なる例示に過ぎず、限定的に解釈してはならない。

## 【 0 2 6 2 】

## 【発明の効果】

以上のように、本発明によれば、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理を検出するための署名データを簡単な構成で、高速に生成することができる。又、その署名データを用いて、デジタルデータに対する不正な処理を簡単な構成で、高速且つ確実に検出することができる。

## 【0263】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの機器によって生成されたかを特定することができる。

## 【0264】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの機器によって生成されたかを特定することができる。

## 【0265】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

## 【0266】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とその機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

## 【図面の簡単な説明】

## 【図1】

本実施例のデジタル画像検証システムについて説明する図。

## 【図2】

本実施例の画像入力装置の基本構成について説明するブロック図。

【図 3】

本実施例の画像検証装置の基本構成について説明するブロック図。

【図 4】

第 1 の実施例の処理手順を説明するフローチャート。

【図 5】

第 1 の実施例における所定の演算処理を説明する図。

【図 6】

第 2 の実施例の処理手順を説明するフローチャート。

【図 7】

第 2 の実施例における J P E G データを表す図。

【図 8】

第 2 の実施例における秘密情報を説明する図。

【図 9】

第 2 の実施例における所定の演算処理を説明する図。

【図 1 0】

第 2 の実施例におけるハッシュ関数演算の第 1 のモードを説明する図。

【図 1 1】

第 2 の実施例におけるハッシュ関数演算の第 2 のモードを説明する図。

【図 1 2】

第 2 の実施例におけるハッシュ関数演算の第 3 のモードを説明する図。

【図 1 3】

第 1 ～第 3 のモードにおける使用される初期値を説明する図。

【図 1 4】

第 3 の実施例の処理手順を説明するフローチャート。

【図 1 5】

第 3 の実施例における秘密情報を説明する図。

【図 1 6】

第 3 の実施例における C B C モードを説明する図。

【図 1 7】

第 3 の実施例における C F B モードを説明する図。

【図 1 8】

第 3 の実施例における O F B モードを説明する図。

【図 1 9】

第 4 の実施例の処理手順を説明するフローチャート。

【図 2 0】

第 4 の実施例における秘密情報を説明する図。

【図 2 1】

第 5、第 6 の実施例の処理手順を説明するフローチャート。

【図 2 2】

画像入力装置と外部装置とを説明する図。

【図 2 3】

第 7 の実施例の処理手順を説明するフローチャート。

【図 2 4】

第 8 の実施例の処理手順を説明するフローチャート。

【図 2 5】

第 9 の実施例の処理手順を説明するフローチャート。

【図 2 6】

第 1 0 の実施例の処理手順を説明するフローチャート。

【図 2 7】

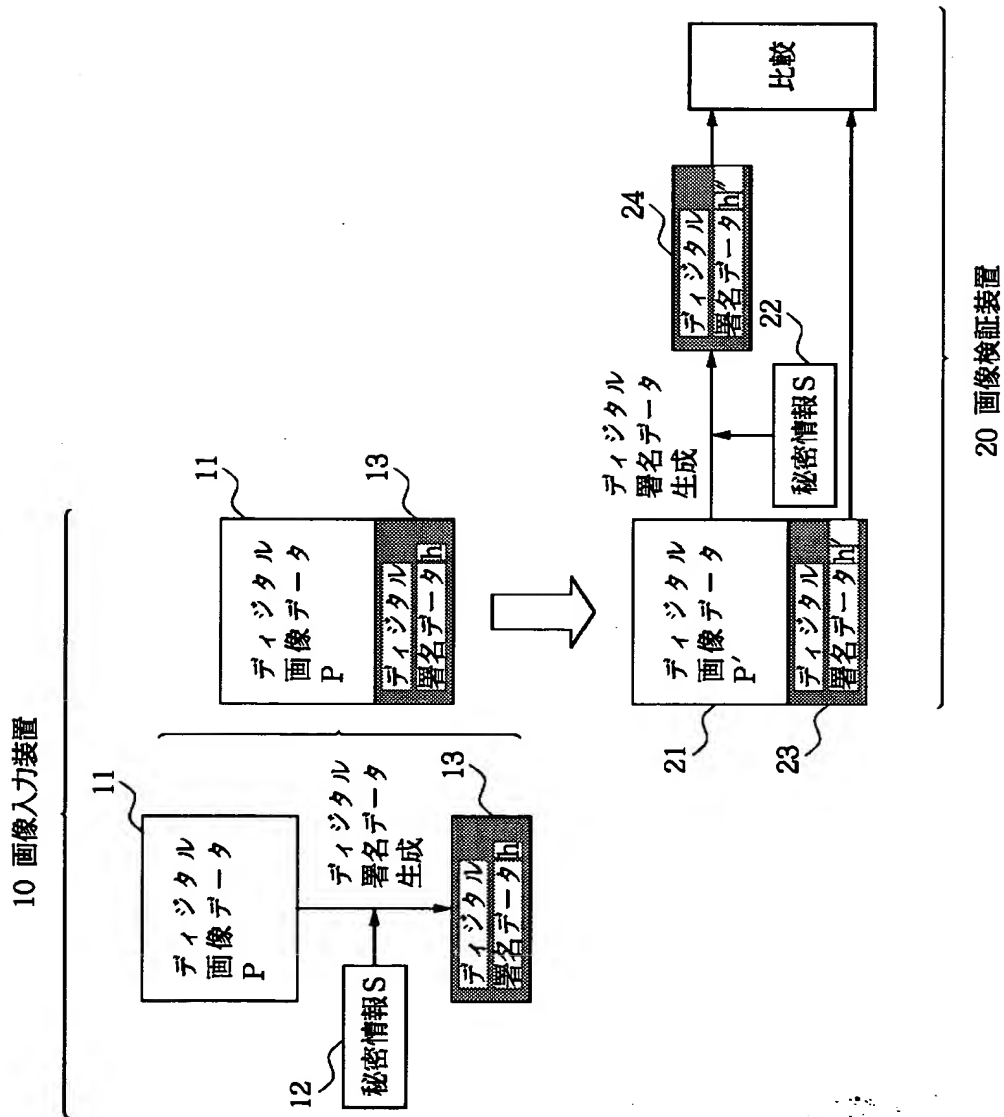
第 1 1、第 1 2 の実施例の処理手順を説明するフローチャート。

【図 2 8】

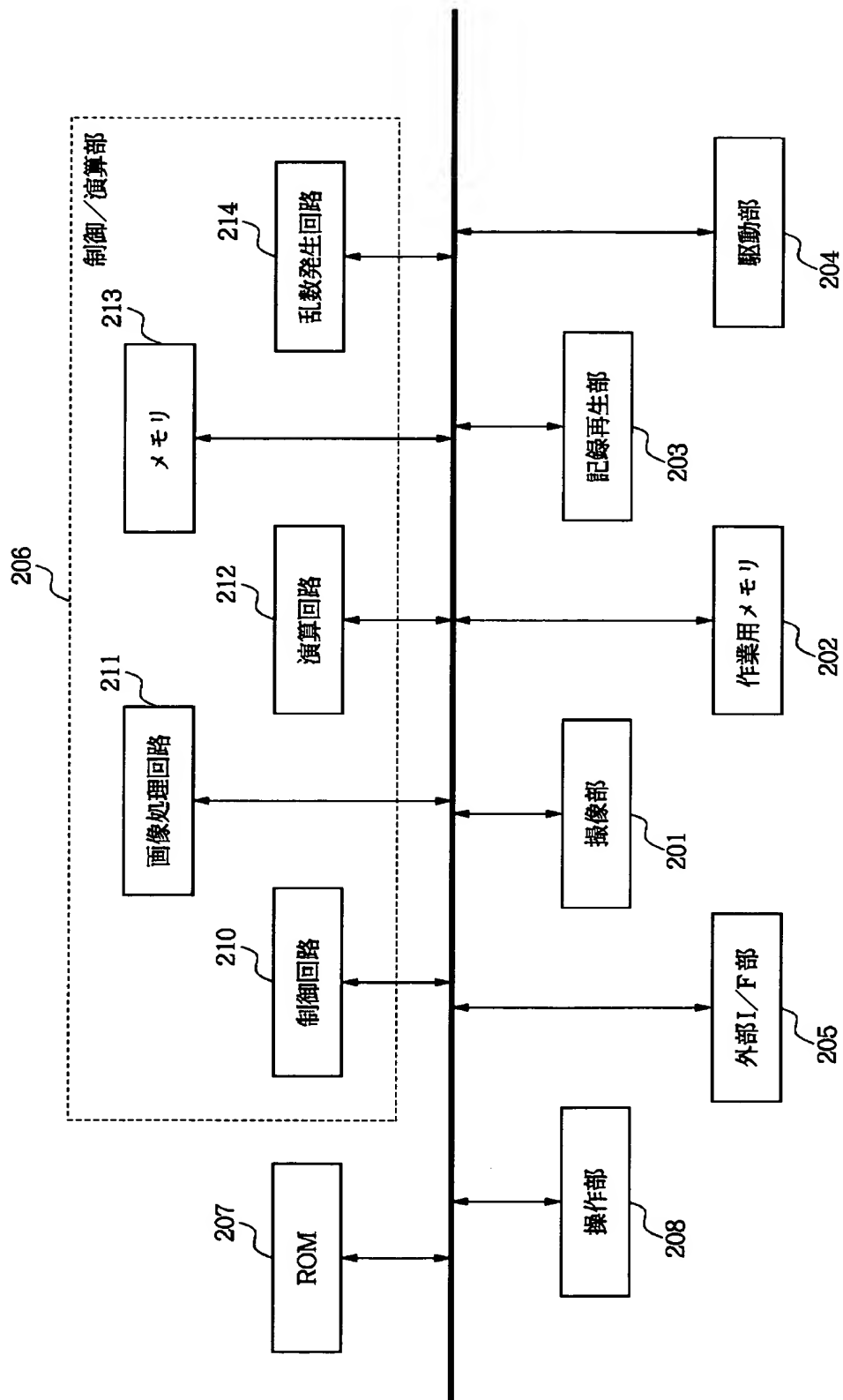
従来のシステムを説明する図。

【書類名】 図面

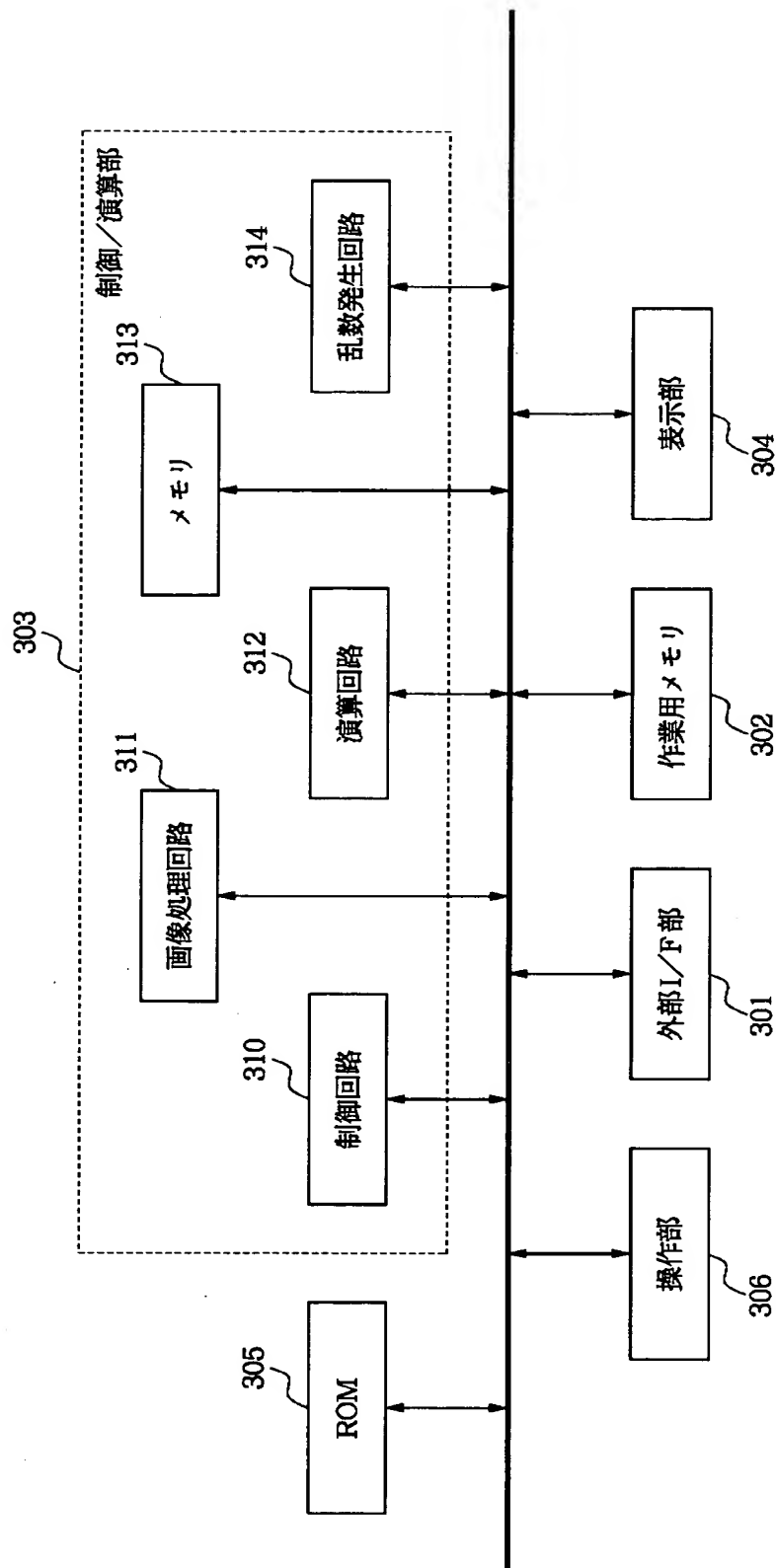
【図 1】



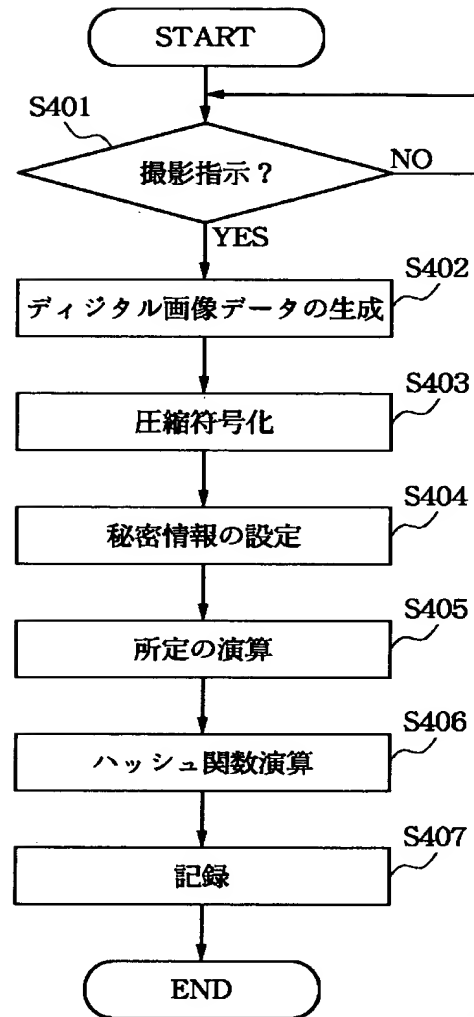
【図 2】



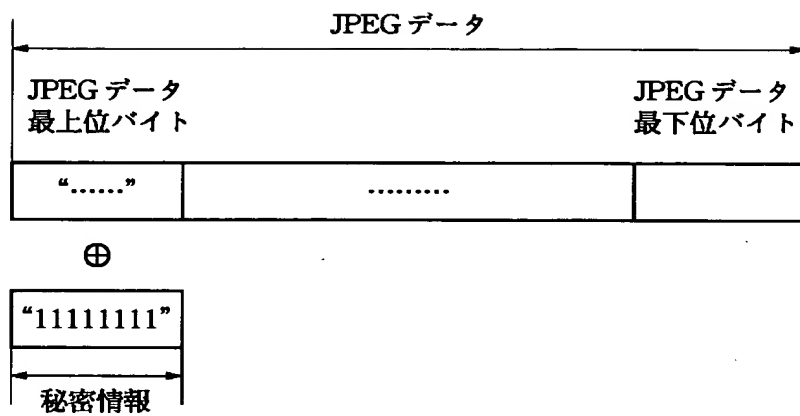
【図3】



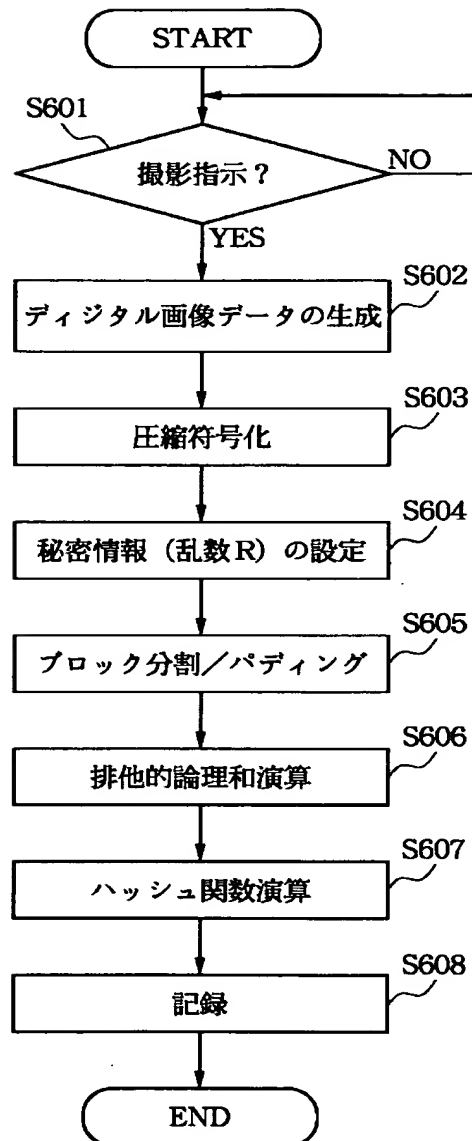
【図 4】



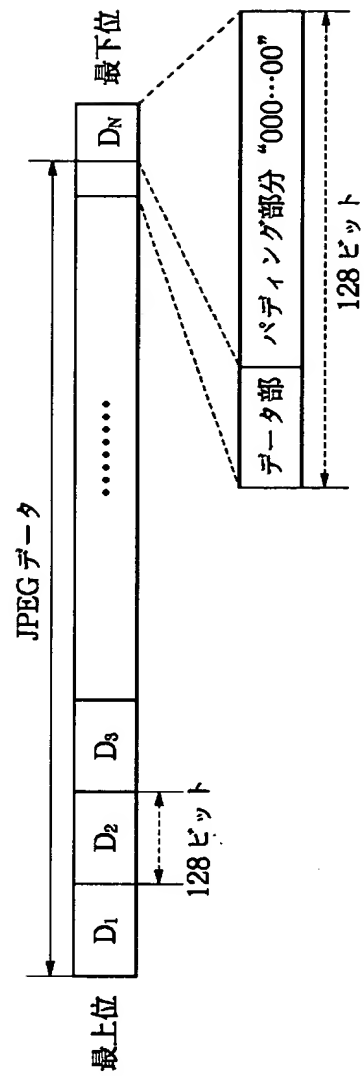
【図 5】



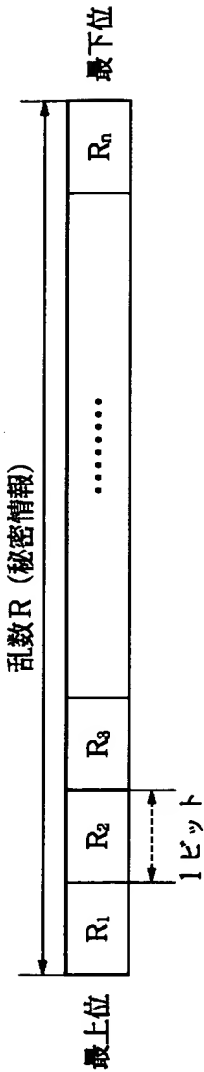
【図 6】



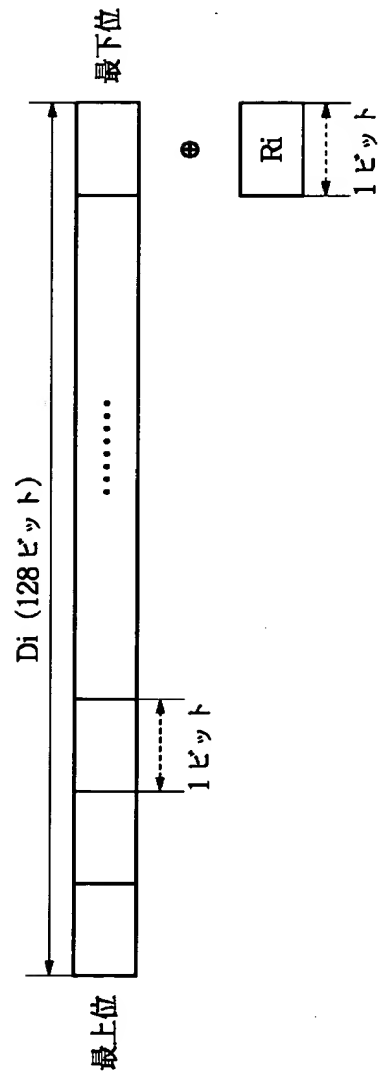
【図 7】



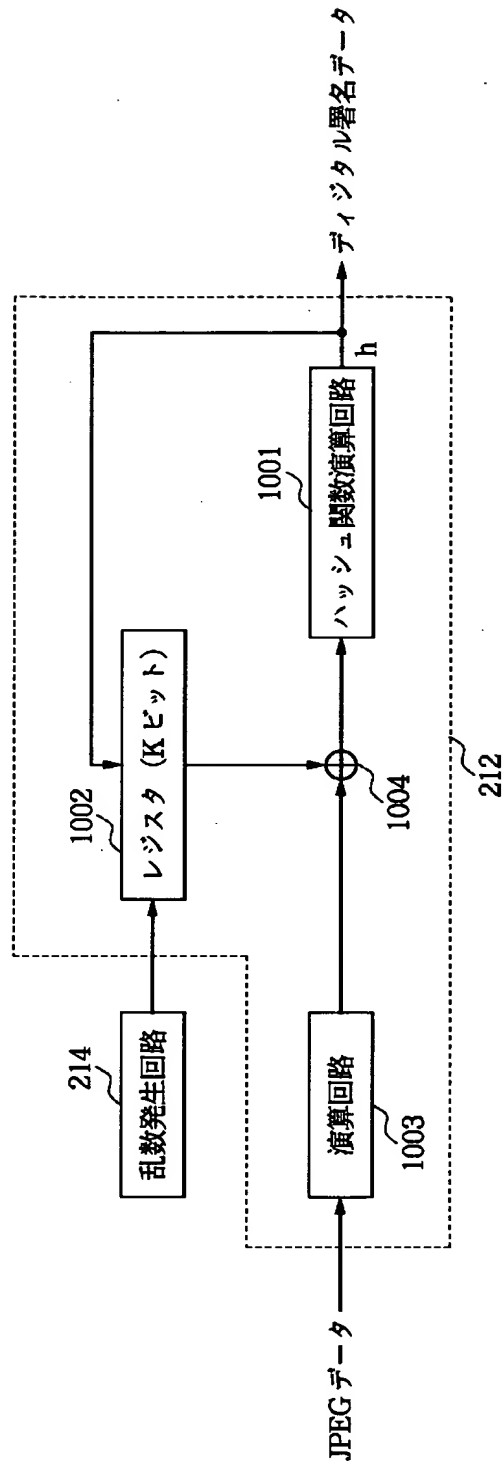
【図 8】



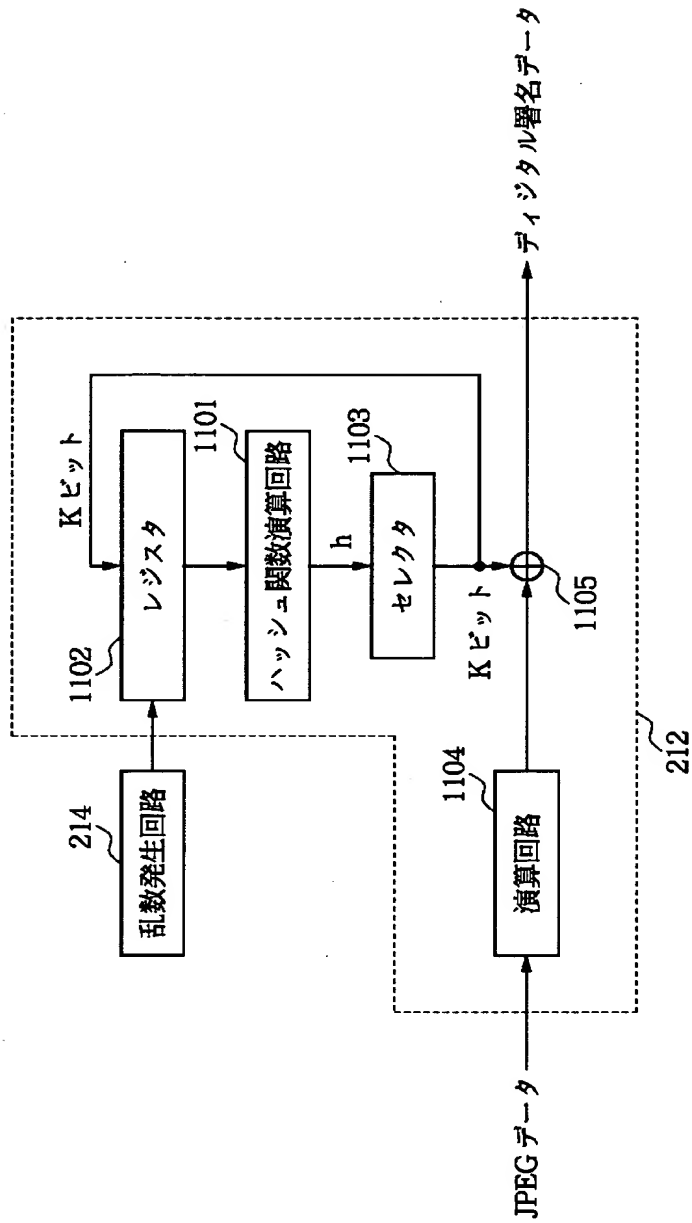
【図 9】



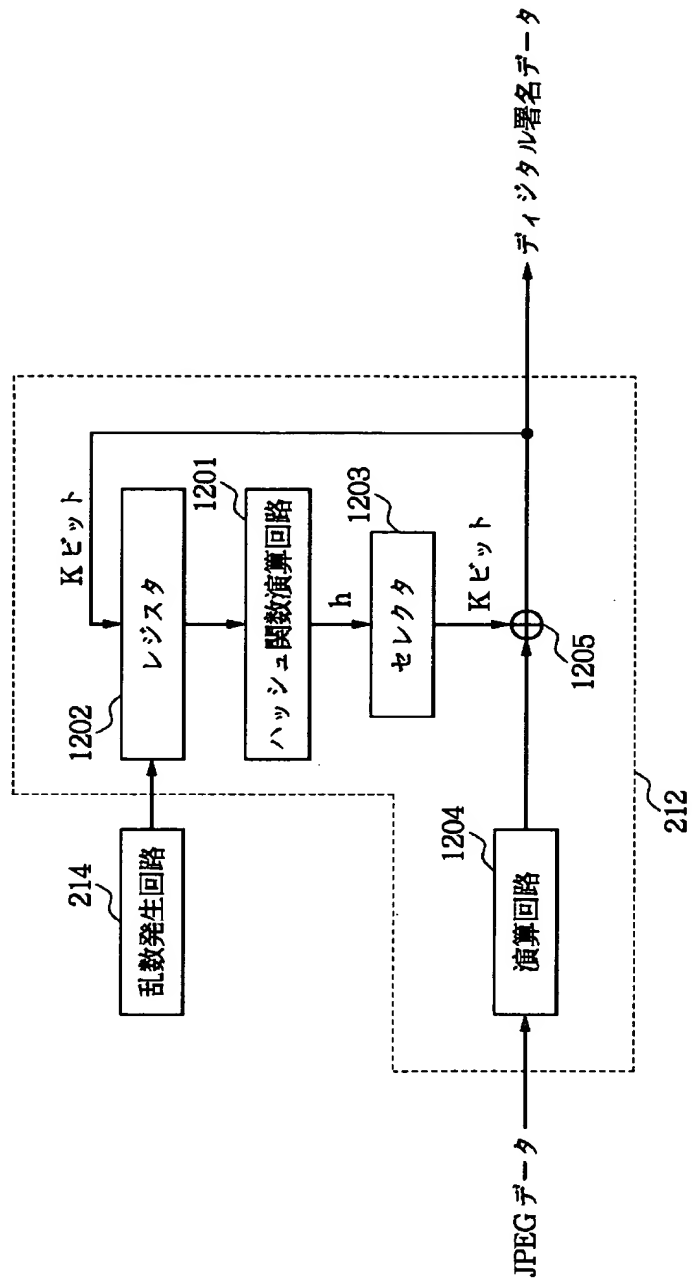
【図 1 0】



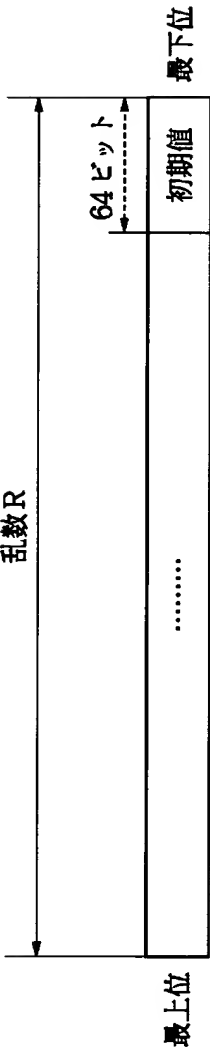
【図 11】



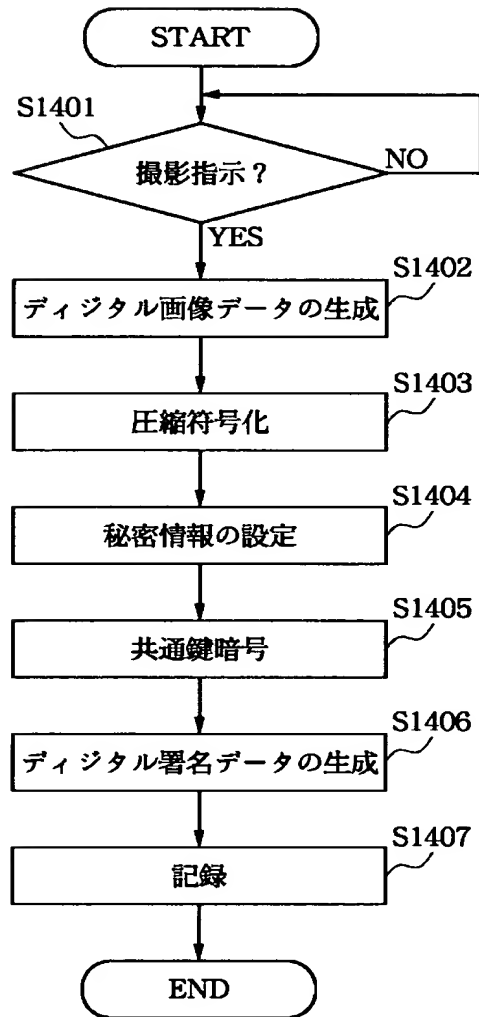
【図 1 2】



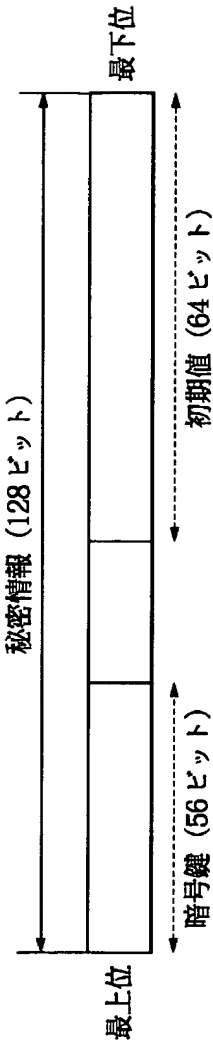
【図 1 3】



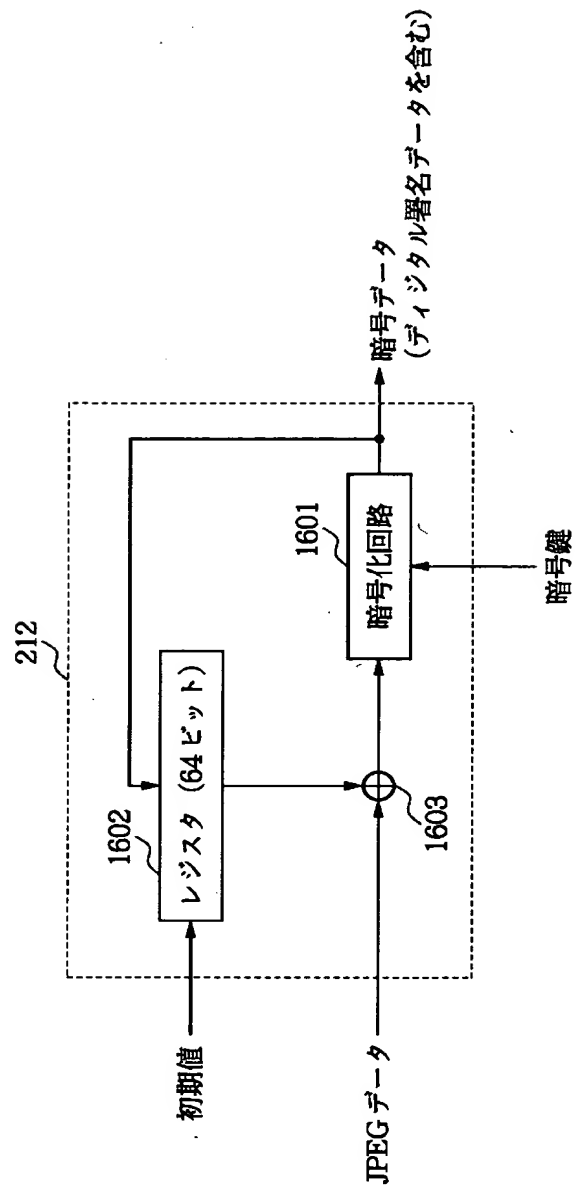
【図 1 4】



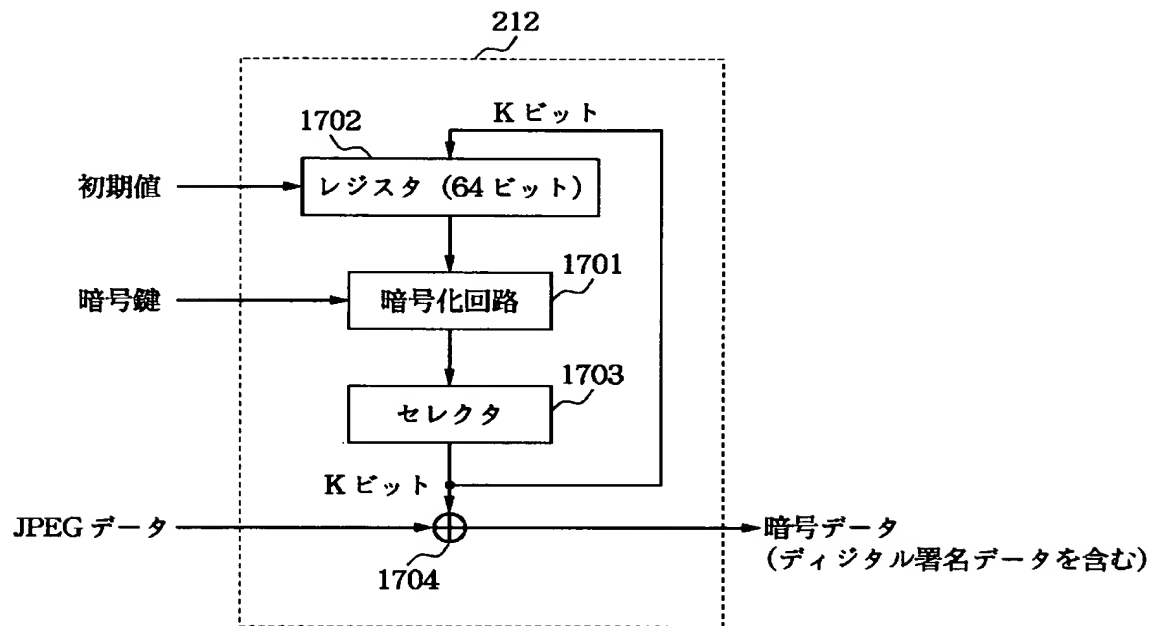
【図 1 5】



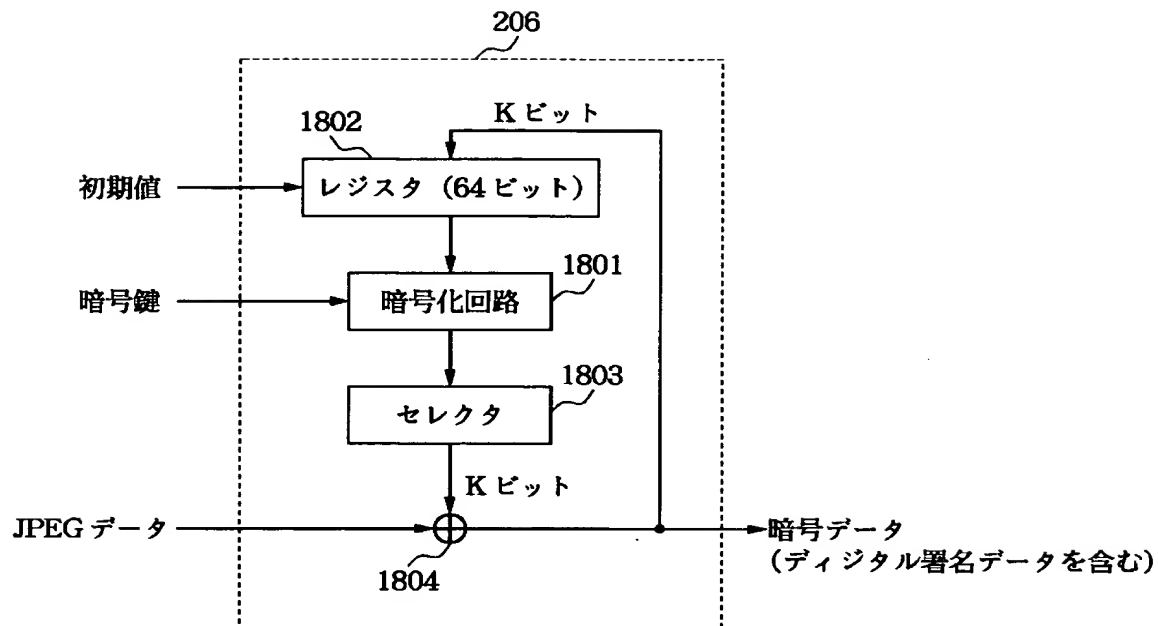
【図 1 6】



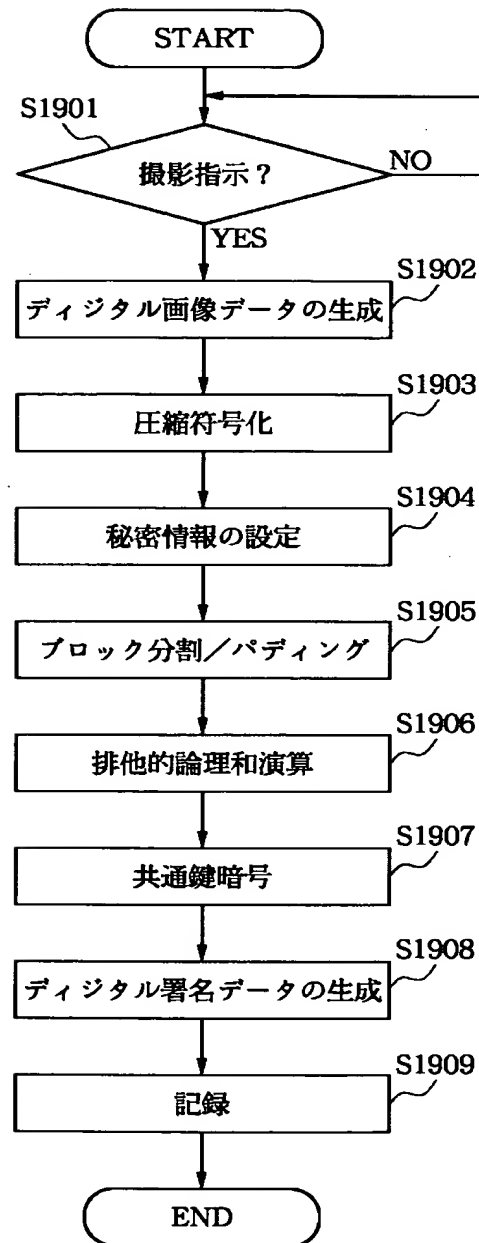
【図 1 7】



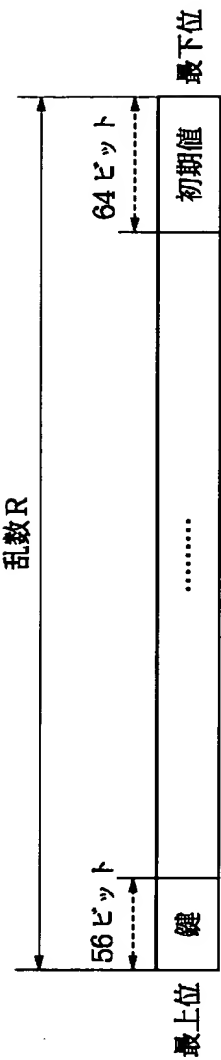
【図 18】



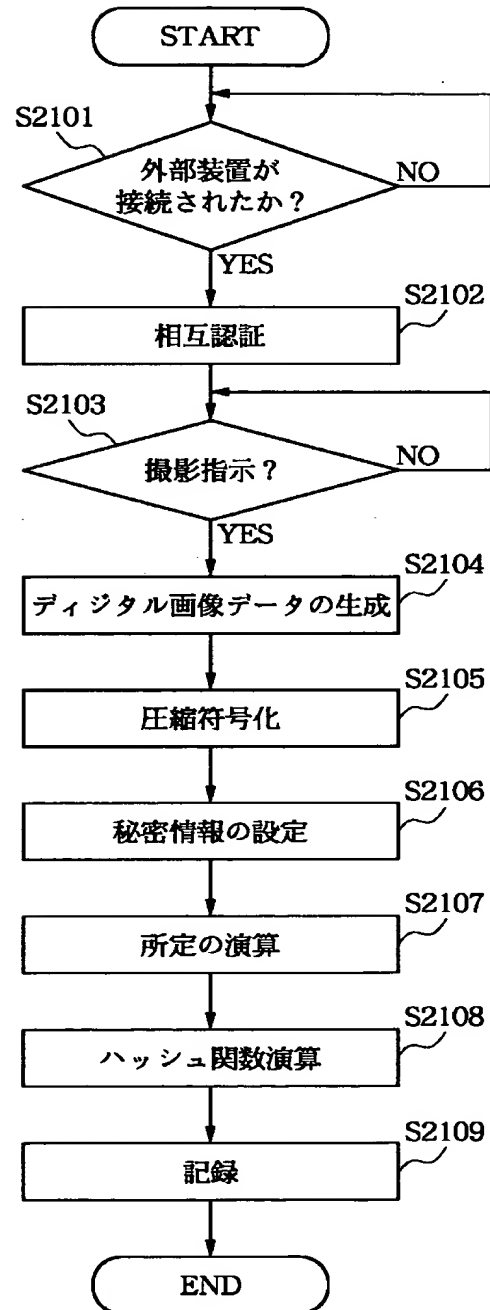
【図 19】



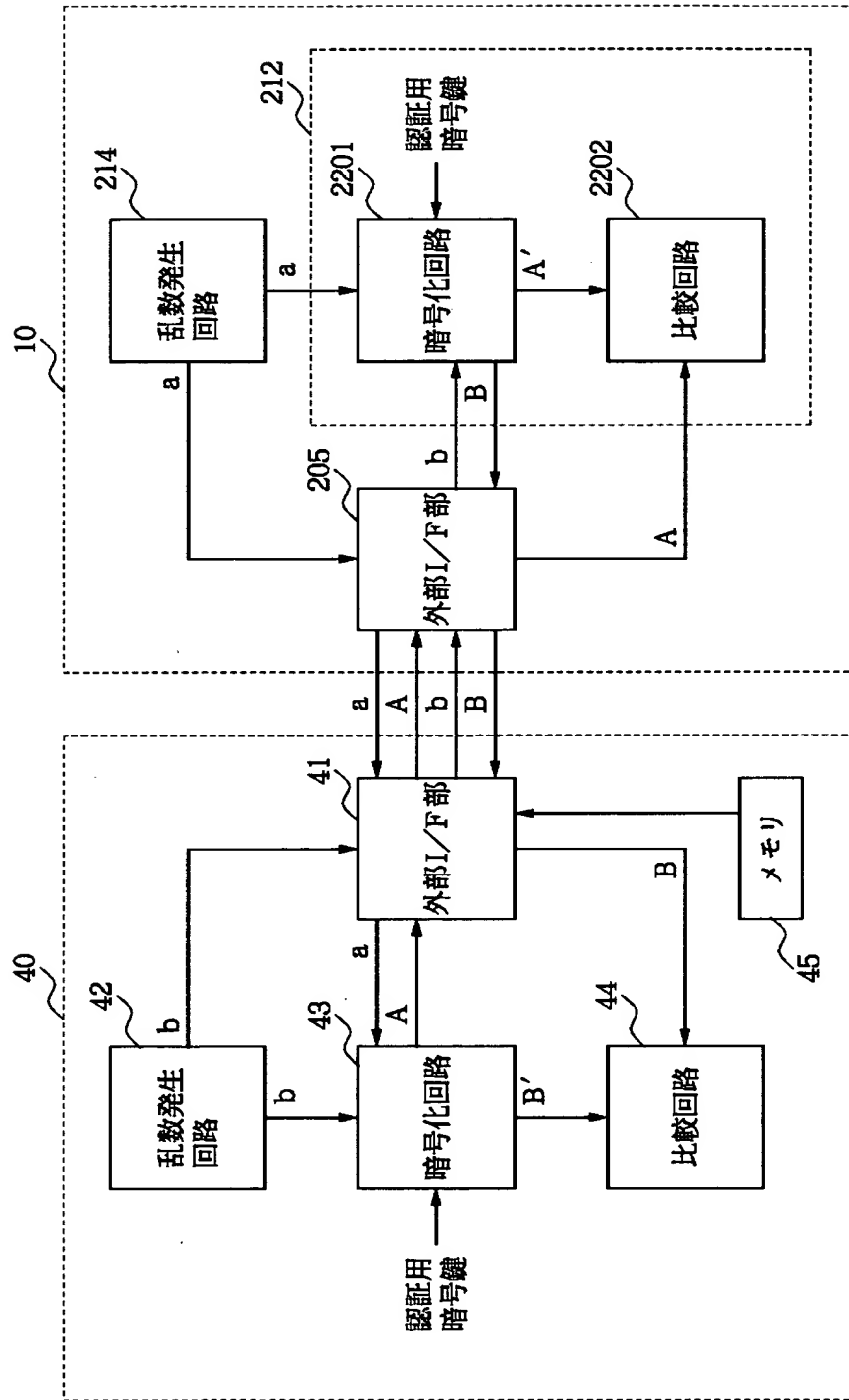
【図 2 0】



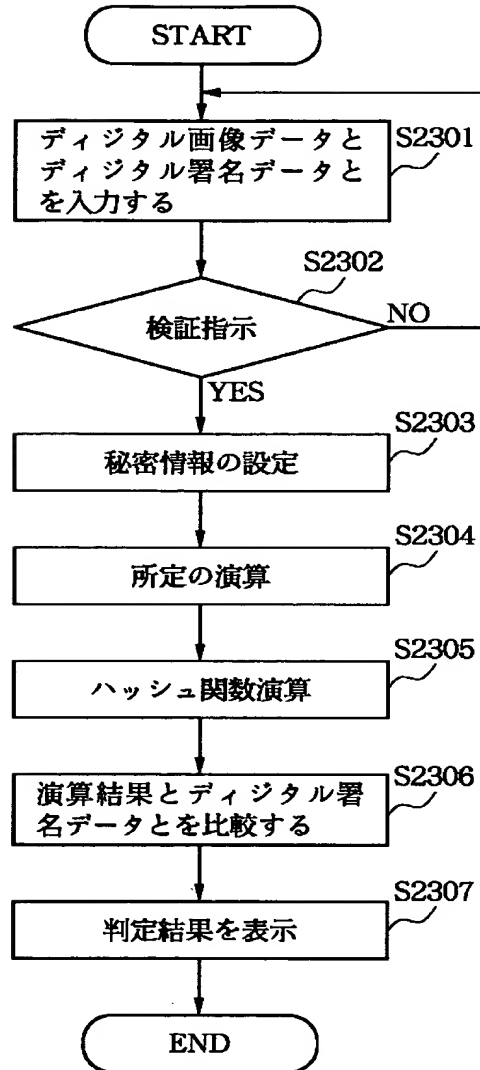
【図 2 1】



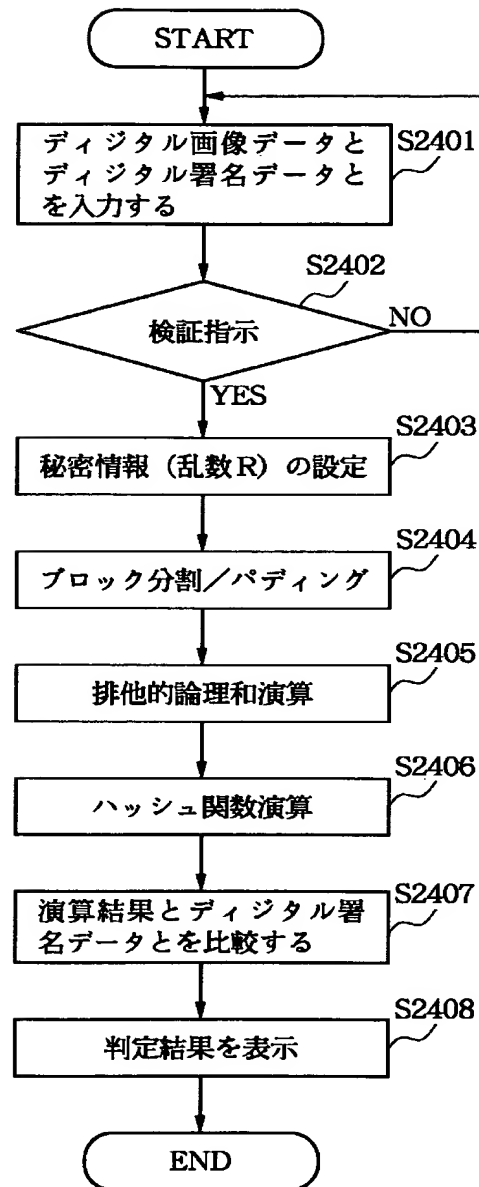
【図 22】



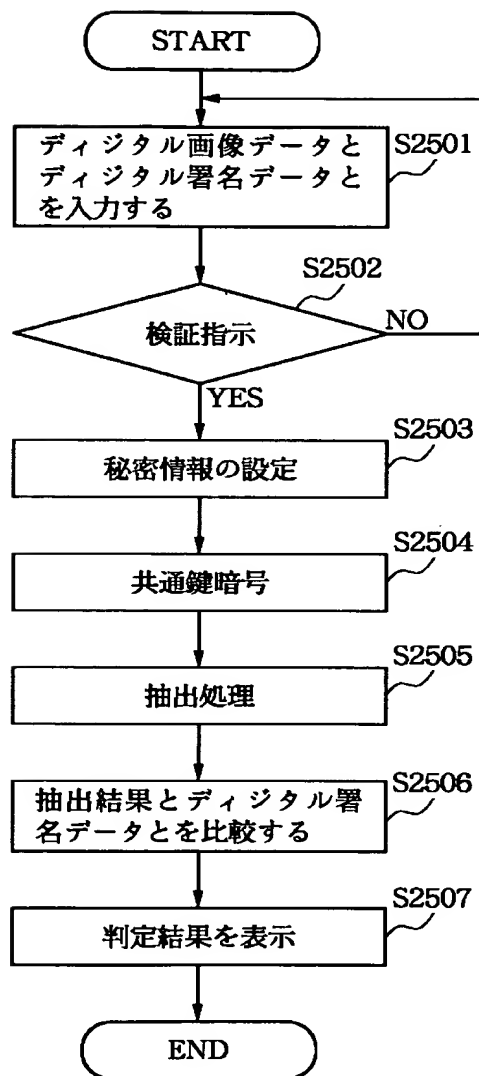
【図 23】



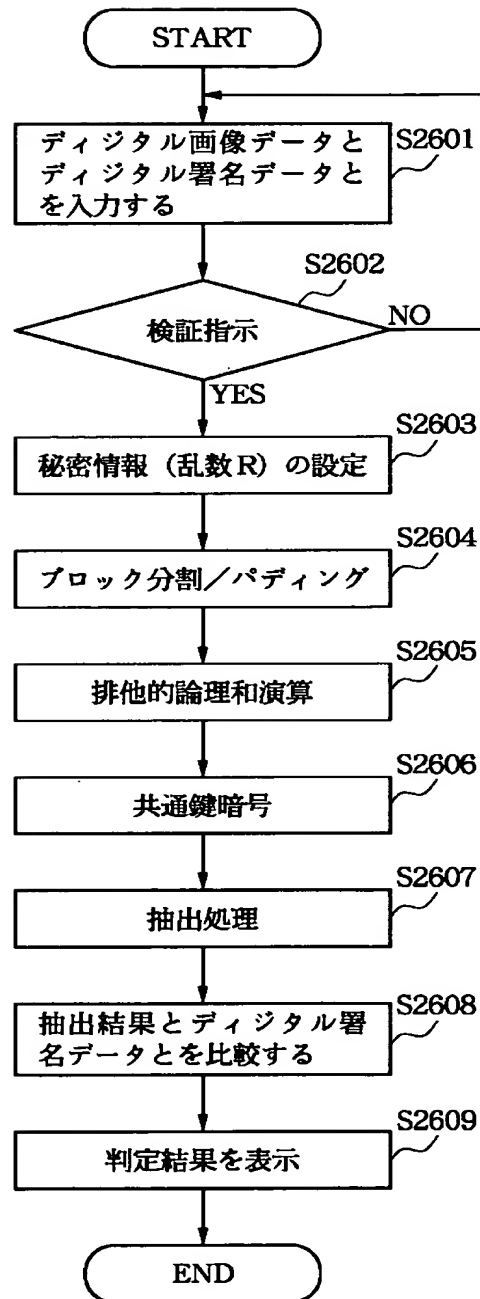
【図 2 4】



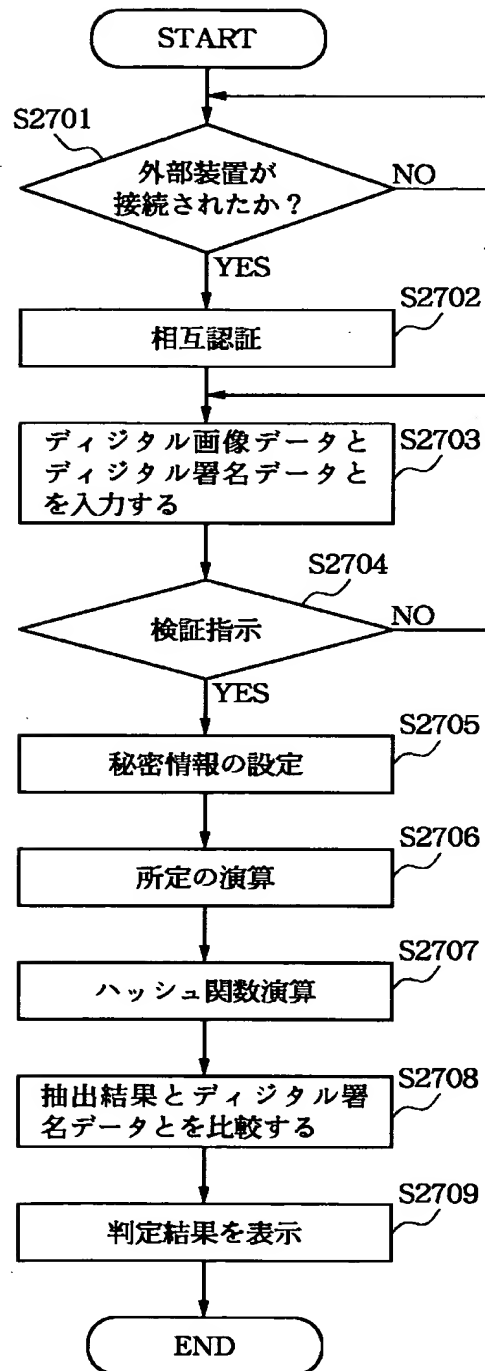
【図 2 5】



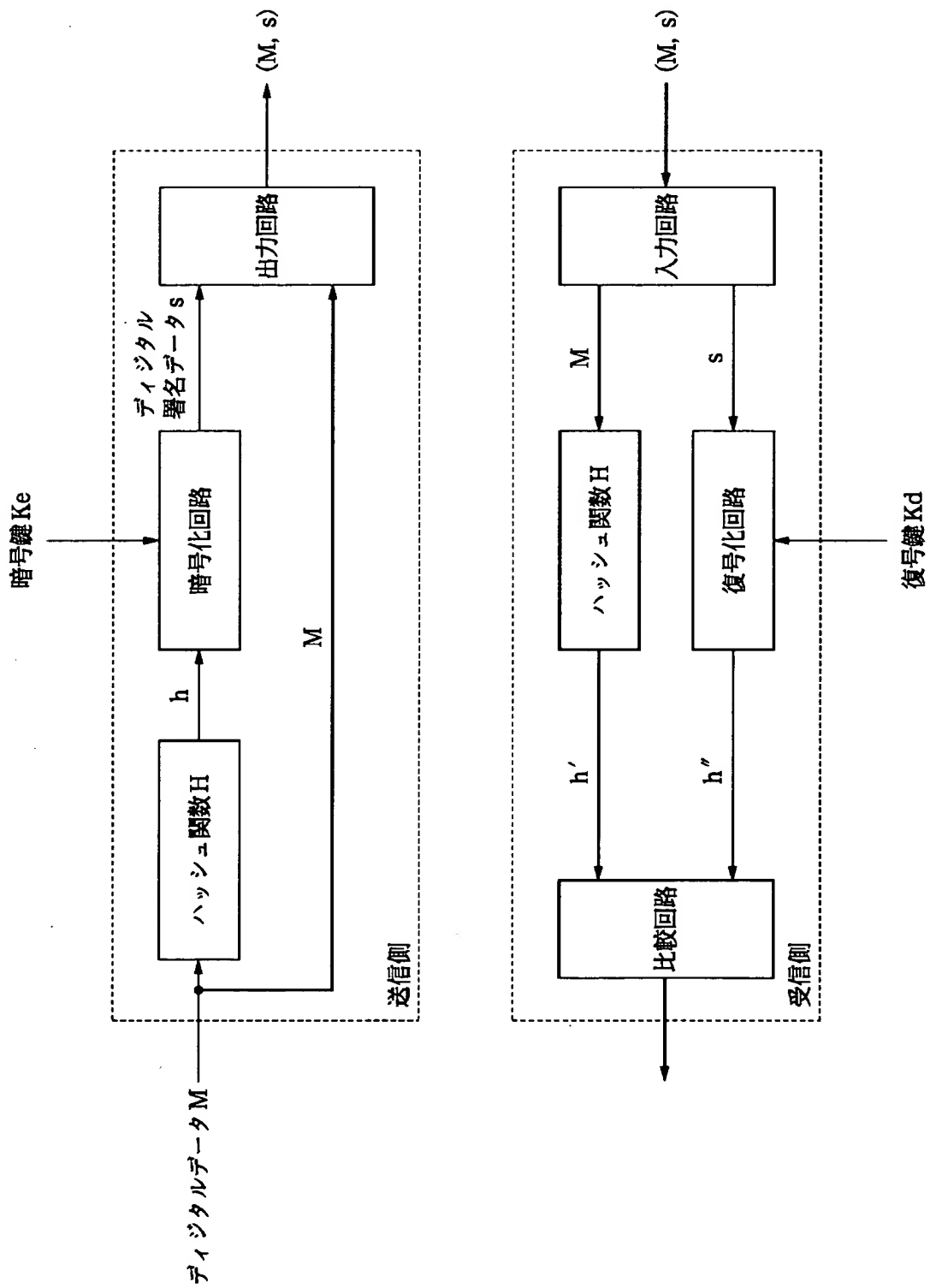
【図 26】



【図 27】



【図 28】



【書類名】            要約書

【要約】

【課題】    デジタルデータの正当性を検証することのできる技術を提供する。

【解決手段】    第 1 の画像処理装置 1 0 は、デジタル画像 1 1 と秘密情報 1 2 とを用いて所定の演算を行い、その演算結果を用いて該デジタル画像に対する不正な処理を検出するため署名データ 1 3 を生成する。第 2 の画像処理装置 2 0 は、そのデジタル画像 1 1 と秘密情報 2 2 とを用いて所定の演算を行い、その演算結果と上述の署名データ 1 3 とを比較してそのデジタル画像 1 1 に対する不正な処理の有無を検出する。

【選択図】            図 1

認定・付加情報

特許出願の番号	特願 2000-057077
受付番号	50000246613
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 3月 7日

<認定情報・付加情報>

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キヤノン株式会社

【代理人】 申請人

【識別番号】 100090538

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

【氏名又は名称】 西山 恵三

【選任した代理人】

【識別番号】 100096965

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

【氏名又は名称】 内尾 裕一

【選任した代理人】

【識別番号】 100110009

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

【氏名又は名称】 青木 康

【選任した代理人】

【識別番号】 100069877

【住所又は居所】 東京都大田区下丸子3-30-2 キヤノン株式会社内

【氏名又は名称】 丸島 儀一

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都大田区下丸子3丁目30番2号  
氏 名 キヤノン株式会社